OFFENSIVE CYBERSPACE OPERATIONS: A GRAY AREA IN CONGRESSIONAL OVERSIGHT

DR. CHRISTOPHER E. BAILEY, SJD*

ABSTRACT

In past 15 years offensive cyberspace operations have become a significant instrument of national power, with state practice ranging from relatively benign intelligence collection to uses of force that threaten international peace and security. Cyberspace operations offer many advantages to the attacker, including the ability to conduct discrete operations that promise a high pay-off at an apparent low-risk. For the defender, there are difficult problems in characterizing an event and identifying the responsible parties. These offensive cyberspace operations raise important questions under international and domestic law concerning the use of force “short of hostilities” in advancing identifiable foreign policy objectives and national security interests of the United States.

Recent changes in U.S. law that have allowed the Department of Defense (“DoD”) and the U.S. Cyber Command (“U.S. CYBERCOM”) broader legal authority to conduct offensive cyberspace operations raise serious problems with executive and congressional oversight. In effect, the 2019 National Defense Authorization Act (“NDAA”), signed into law by President Donald Trump on August 13, 2018, muddies the traditional distinctions between Title 10 (Armed Forces) and Title 50 (War and National Defense) authorities, which allows the DoD to conduct coercive and covert actions—to “defend forward” through “persistent engagement”—that it considers “short of hostilities.” This authority creates a risk that DoD would commit an internationally wrongful act, such as a use of force in violation of the Charter of the United Nations, that would jeopardize important national interests. Thus, Congress should act to require pre-operational presidential approval for specified activities, define key

* Dr. Christopher E. Bailey is an Associate Professor at the National Intelligence University in Bethesda, Maryland specializing in national security law, international law, and professional ethics. He is also an adjunct instructor in the Master of Science in Cyber Security program at the University of Charleston (West Virginia). Dr. Bailey is licensed to practice law in California and the District of Columbia, and is a member of the American Society of International Law. He has an LLM degree in National Security & U.S. Foreign Relations Law, as well as a SJD degree in International and Comparative Law, from the George Washington University School of Law. All statements of fact, analysis, or opinion are the author’s and do not reflect the official policy or position of the National Intelligence University, the Department of Defense or any of its components, or the U.S. government.
terminology used in the statute and by DoD, and reconsider the need for prior notification to the congressional oversight committees. Such changes would allow for prompt U.S. action against on-going threats, but also reduce the overall risk that the country would commit an internationally wrongful act.

CONTENTS
I. THE CYBER DOMAIN & THE FUTURE OF 21ST CENTURY CONFLICT ..........242
II. CYBER USES OF FORCE UNDER U.S. LAW ..................................................255
   A. Public Policy Concerns .................................................................256
   B. Constitutional Law .................................................................257
   C. Statutory Law ...........................................................................261
   D. Executive Order 12333, United States Intelligence Activities ....267
   E. Conclusions on U.S. Law .............................................................269
III. CYBER USES OF FORCE UNDER INTERNATIONAL LAW ..................270
   A. Uses of Force Under Charter Law ...............................................270
   B. Cyber Uses of Force .................................................................274
   C. Accountability for Illegal Uses of Force .......................................277
   D. The Application of International Humanitarian Law to Cyber Operations .................................................................279
   E. Conclusions on International Law ................................................283
FINDINGS AND IMPLICATIONS .................................................................283
I. THE CYBER DOMAIN & THE FUTURE OF 21ST CENTURY CONFLICT

Offensive cyberspace operations, including clandestine collection, exploitation and attack, are likely to remain an important means and method in international relations over the coming decades. Cyber warfare offers an attacker the important advantage of remote operations, leaving the victim with the problem of characterizing the event as a violation under domestic or international law, and with untangling the complex intelligence involving source attribution. In the case of technologically advanced states, such as the United States (“U.S.”) or Israel, there are increased intelligence and planning requirements, but a reduced risk of friendly casualties (as compared to physical operations). Most importantly, if the victim cannot properly characterize the event or identify the perpetrators, then the attacker achieves discrete strategic objectives without risking a retaliatory response. Both clandestine and covert cyber actions can, therefore, perform a useful role in furthering U.S. national security interests, provided that such actions comply with relevant domestic law to include appropriate executive and congressional oversight, are conducted consistent with fundamental principles of international law, and fall below a certain level of severity based upon either the nature of the target or the degree of harm caused.

Several recent instances of cyber operations indicate that offensive cyberspace operations will likely be a staple in future international armed conflict. Examples include Israel’s possible installation of a secretly kill-switch to destroy Syrian air defenses prior to its 2007 bombing of a nuclear reactor, Russia’s likely deployment of a patriotic “cyber mob” for a 2007 attack on Estonia, the possible joint U.S.-Israeli use of a thumb drive to facilitate the 2010


2 Under Common Article 2, of the Geneva Conventions of 1949, an international armed conflict is defined as a “declared war or any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them.” Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces of the Field art. 2, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Geneva Convention for the Amelioration of the Condition of Wounded, Sick, and Shipwrecked Members of Armed Forces at Sea art. 2, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Geneva Convention Relative to the Treatment of Prisoners of War art. 2, August 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Geneva Convention Relative to the Protection of Civilian Person in Time of War art. 2, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287. This article is concerned with the use of covert cyber operations as a means and method of armed conflict by nation-states, to include actions through proxies against other states.


4 A Look at Estonia’s Cyber Attack in 2007, ASSOCIATED PRESS, July 8, 2009,
Stuxnet attack against Iranian nuclear facilities, and the Russian interference in the 2016 U.S. general election. In fact, offensive cyberspace operations conducted under conditions of secrecy can be an useful force multiplier, for a government seeking either to avert conflict (e.g., anticipatory self-defense) or to facilitate operations during war. In this article, cyber operations are understood as military-intelligence operations using computers or computer networks either to target another or to use that other computer or computer network as a means by which damage or injury is caused to an adversary. Cyber operations, especially those that impair or degrade an adversary’s systems, will likely remain a preferred method of attack against foreign adversaries because of problems that victims typically experience in characterizing an event and in

http://www.nbcnews.com/id/31801246/ns/technology_and_science/security/t/look-estonias-cyber-attack/[https://perma.cc/E523-XUVN]. After Estonia proposed moving a Soviet War Memorial, Estonian websites, to include sites owned by the government, banks, and media outlets, were targeted through Distributed Denial of Service (DDoS) attacks in April-May 2007. Moscow denied responsibility, even though much of the web traffic originated from Russia and there was some evidence of government support. While these attacks could have had state sponsorship, it equally possible that the attacks were the work of a “cyber mob” that was angry with Estonia. Nonetheless, a broad based, coercive attack like this can have a psychological chilling effect on both a government and its people; an attack like this could be construed as an act of cyber terrorism. Michael L. Gross et al., Cyber Terrorism: Its Effects on Psychological Well-Being, Public Confidence, in by, BOMBS, AND SPIES: THE STRATEGIC DIMENSIONS OF OFFENSIVE CYBER OPERATIONS 235 (Herbert Lin & Amy Zegart ed., 2018).


7 Cyber operations can be either offensive, that is attacking an adversary’s system to destroy, degrade or impair its effectiveness or capability, or defensive, that is protecting one’s own systems from attack by an adversary. Some cyber operations, such as the insertion of a virus or program that can be activated at a later date, may also be viewed as preparation for a subsequent attack. There is some evidence, for example, that the U.S. government may have made an earlier penetration of the Chinese network that connects North Korea to the rest of the world, allowing the emplacement of malware that could have provided an “early warning radar” for the impending attack on Sony. David E. Sanger & Marvin Fackler, N.S.A. Breached North Korean Networks Before Sony Attack, OFFICIALS SAY, N. Y. TIMES, Jan. 18, 2015, http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?_r=0.
attributing the attack to state-sponsorship.8 Offensive cyberspace operations raise important national security and foreign policy concerns that implicate U.S. and international law, especially as global political, defense, economic, and law enforcement activity increases its reliance on computer systems.9

Offensive cyberspace operations range from the relatively benign exploitation of a zero day vulnerability,10 which enables a Distributed Denial of Service

---

8 This article uses the definition of covert action found in 50 U.S.C. § 3093 (e): the term “covert action” means an activity or activities that are “designed to influence the political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly ….” It is useful to distinguish covert actions from clandestine activities: with a covert action, the act itself will often be known to or observable by the adversary, even if sponsorship cannot be established; with a clandestine activity, the adversary is usually not witting to either the act or the actor (e.g., a classic example of clandestine activity involves espionage). On one hand, the Soviet Union had to know that someone had provided advanced weapons to the Afghan mujahideen in the 1980’s, but could not necessarily have established that the weapons had come from the United States and Saudi Arabia. On the other hand, when the Central Intelligence Agency (CIA) conducts espionage operations in a foreign capital, it doesn’t want the foreign government to know about either the passage of material or the spy himself. See Kirsten Lundberg, Politics of a Covert Action: The U.S., the Mujahideen, and the Stinger Missile, Kennedy School of Government Case Program (1999).

9 Numerous commentators have raised the prospect of cyber war as a pressing issue for national security professionals over the past 20 years. See, for example, CYBERWAR 2.0: MYTHS, MYSTERIES AND REALITY (Alan D. Campen & Douglas H. Heath, eds., 1998) (offering a range of essays regarding the impact of cyber on strategy and diplomacy, commerce, information operations and intelligence), and FRANKLIN D. KRAMER ET AL., CYBERPOWER AND NATIONAL SECURITY (2009) (this volume of essays provides a broad view of the cyber domain and the complex issues that policymakers should address in developing cyber power as an effective component in U.S. national security strategy). Currently, the DoD sees a need to “assertively defend our interests in cyberspace below the level of armed conflict and ensure the readiness of our cyberspace operators to support the Joint Force in crisis and conflict.” U.S. DEP’T OF DEFENSE, DEPARTMENT OF DEFENSE CYBER STRATEGY (SUMMARY) 2 (2018). The DoD has defined a strategic approach “based on mutually reinforcing lines of effort to build a more lethal force; compete and deter in cyberspace; expand alliances and partnerships; reform the Department; and cultivate talent.” Id. at 4. Finally, in September 2018, the Trump administration released “a fully articulated cyber strategy” based upon four pillars: Protect the American People, the Homeland, and the American Way of Life (Pillar I); Promote American Prosperity (Pillar II); Preserve Peace Through Strength (Pillar III); and Advance American Influence (Pillar IV). EXEC. OFFICE OF THE PRESIDENT, NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA (Sept. 2018), https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/ [https://perma.cc/33TV-7H96], (last visited July 7, 2020). Pillar III cites increasingly challenges to U.S. security and economic interests in cyberspace and claims that “[this] now-persistent engagement in cyberspace is already altering the strategic balance of power.” Id. at 20.

10 A zero day vulnerability refers a newly discovered software vulnerability; in other words, a software developer has not yet created a patch or an update to fix the issue. This
means that software developers have “zero days” to address the problem that has just been exposed. Thus, a cyber attacker using such previously unknown vulnerabilities can have an operational advantage over a cyber defender. Steven M. Bellovin et al., Limiting the Undesired Impact of Cyber Weapons, in BYTES, BOMBS, AND SPIES: THE STRATEGIC DIMENSIONS OF OFFENSIVE CYBER OPERATIONS 265, 267 (Herbert Lin & Amy Zegart ed., 2018).

A DDoS attack is a “technique that employs two or more computers, such as bots of a botnet, to achieve a denial of service from a single or multiple targets.” TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 565 (Michael N. Schmitt, ed., 2d ed. 2017) [hereinafter TALLINN MANUAL]. A botnet is defined as a network of compromised computers (the bots) that are remotely controlled by an intruder to conduct cyber operations; the use of a botnet to attack an adversary typically results in a flooding of the attacked systems with messages that overload those systems and result in a denial of service. Id. at 563. The dual use nature of many key facilities and systems raises difficult issues concerning the principle of distinction, § III (d) infra, and on an attack on such targets could be viewed by the victim state.

The term “SCADA” refers to the supervisory control and data acquisition systems used in modern industrial control systems that are controlled by computers and automate many, if not all, management processes. An attack against such a system could have a major crippling impact on public utilities over large areas with severe second and third order effects resulting from an interruption of services. TALLINN MANUAL, supra note 11, at 567.

The term “Critical Infrastructure” is defined in U.S. law as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” Critical Infrastructures Protection Act of 2001, 42 U.S.C. § 5195c(e) (2001). See also Exec. Order No. 13800, 82 Fed. Reg. 22391 (May 16, 2017).


The evidence suggests that Pyongyang conducted a malicious cyber operation against Sony over production of a movie that portrayed North Korea’s leader in an unflattering light. Subsequently, within days of the attack on Sony, the hacker group Anonymous announced several retaliatory DDoS attacks that resulted in nation-wide blackouts. If true, North Korea’s initial violation of U.S. sovereignty could have provided the United States with the moral and legal justification for a proportionate response. In any case, the possible use of a proxy group to conduct a covert attack against North Korea also illustrates its utility: if Pyongyang is
the use of proxies could be used to warn an adversary about the risk of conducting a cyber-attack against the United States.\textsuperscript{17} White House and senior Russian leaders have also highlighted the gravity of the situation; both countries have expressed the need for stronger cyber defenses to protect against cyber-attacks from foreign state and non-state actors.\textsuperscript{18} Indeed, the likely Russian interference in the 2016 presidential elections demonstrate that the international community faces a pernicious security threat through the use of social media platforms by state-supported actors.\textsuperscript{19}

\textsuperscript{17} In general terms, nation-states can be held responsible for their own actions, as well as for any actions carried out by proxies under their direction and control. Harold Hongju Koh, Legal Adviser, U.S. Dep’t of State, Remarks at the U.S. CYBERCOM Inter-Agency Legal Conference, (Sept. 18, 2012), https://2009-wide.open祢.org/the-press/releases/remarks/887924.htm.

\textsuperscript{18} EXEC. OFFICE OF THE PRESIDENT, NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA (Sept. 18, 2018) https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (last visited July 23, 2019); EXEC. OFFICE OF THE PRESIDENT, INTERNATIONAL STRATEGY FOR CYBERSPACE (May. 2011), [https://perma.cc/EH9D-P23E]; Sergei Ptichkin, Russia Building a Unified System to Defend Against Cyber Attacks, RUSS. BEYOND THE HEADLINES (Nov. 26, 2014), http://rbth.com/science_and_tech/2014/11/26/russia_building_a_unified_system_to_defend_against_cyber_att_41719.html [https://perma.cc/3NUQ-QAP5]. The 2017 U.S. National Security Strategy recognizes the importance of cybersecurity and the need to defend ourselves “within the framework of international law.” EXEC. OFFICE OF THE PRESIDENT, NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 41 (December 2017). Earlier, in 2007-08, the North Atlantic Treaty Organization (NATO) had recognized the growing threat of cyber operations and established a Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia with a “mission to enhance the capability, cooperation and information sharing among NATO, its member nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation.” NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLECE (last visited July 23, 2019), https://ccdcoe.org/index.html. The NATO Centre has been at the forefront of legal research and scholarship on the application of international humanitarian law (IHL) to cyber operations, to include the 2017 publication of the influential TALLINN MANUAL. This influential manual, prepared by an eminent group of experts, can be considered as a restatement of international humanitarian law as applied to cyber operations. TALLINN MANUAL, supra note 11.

Accordingly, a 2018 comprehensive cyber strategy rolled out by the Trump Administration indicates that the United States will undertake offensive cyberspace operations against foreign adversaries.\textsuperscript{20} Initially, President Donald Trump signed the 2019 National Defense Authorization Act ("NDAA") into law on August 13, 2018. The 2019 NDAA further militarizes cyberspace by authorizing the Department of Defense ("DoD") to conduct a range of clandestine military cyber operations—including when such actions would fall short of hostilities or would occur in areas in which hostilities are not occurring\textsuperscript{21}—as a "traditional military activity" pursuant to the covert action statute.\textsuperscript{22} President Trump subsequently rescinded Presidential Policy Directive (PPD) 20, the interagency legal and policy process that had been initiated by President Barack Obama and used for "green-lighting" cyber-attacks.\textsuperscript{23} A House of Representatives conference report noted that the DoD had faced interagency problems in obtaining mission approval for cyber operations, and found that the

\textsuperscript{20} Exic. Office of the President, National Cyber Strategy of the United States of America 20-21 (Sept. 2018). See also Dan Lohrmann, New National Cyber Strategy Message: Deterrence Through U.S. Strength, Government Tech. (Sept. 29, 2018), https://www.govtech.com/blogs/lohrmann-on-cybersecurity/new-national-cyber-strategy-message-deterrence-through-us-strength.html [https://perma.cc/S5UL-VP2] (last visited July 23, 2019). This is also supported by the DoD’s 2018 Cyber Strategy, currently publicly-available only in an official summary document. U.S. Dep’t of Defense, Department of Defense Cyber Strategy (Summary) 3 (2018) This strategy focuses on five—primarily defensive—cyberspace objectives with five supporting lines of effort. This document states that the DoD “will conduct cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict. We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict.” Id. at 1 (emphasis added).


“Congress affirms that [clandestine military cyber activities or operations in cyberspace], when appropriately authorized, include the conduct of military activities or operations in cyberspace short of hostilities (as such term is used in the War Powers Resolution . . . or in areas in which hostilities are not occurring, including for the purpose of preparation of the environment, information operations, force protection, and deterrence of hostilities, or counterterrorism operations involving the Armed Forces of the United States.” Id.

\textsuperscript{22} 10 U.S.C § 394(c).

DoD had been challenged by “the perceived ambiguity as to whether clandestine military activities and operations, even those short of cyber-attacks, qualify as traditional military activities as distinct from covert actions requiring a Presidential Finding.”24 Senator Mike Rounds (D-SD), a member of the Senate Armed Services Committee and chairman of the Cybersecurity Subcommittee, later remarked that PPD-20 had “virtually paralyzed the conduct of offensive operations by U.S. Cyber Command outside of armed conflict.”25 To remedy this problem, Congress authorized an increased range of offensive cyberspace operations, no doubt “unleashing” U.S. Cyber Command (“U.S. CYBERCOM”) from its defensive shackles to conduct a broader range of defensive and offensive operations.26

This broad vesting of authority from Congress to the Secretary of Defense leaves many unanswered questions about the reach of its new operational authority as well as oversight by Congress and the Executive.27 First, one must distinguish among clandestine collection, cyber exploitation, sensitive military

26 The U.S. Cyber Command (U.S. CYBERCOM) is a unified combatant command collocated with the National Security Agency at Fort Meade, Maryland. According to the DoD, the U.S. CYBERCOM “consolidates [cyber] authorities in terms of the direct synchronization of resources, training, as well as the operational planning and execution.” Katie Lang, Cybercom Becomes DoD’s 10th Unified Combatant Command, DoDLive(May 3, 2018), http://www.dodlive.mil/2018/05/03/cybercom-to-become-dods-10th-unified-combatant-command/ [https://perma.cc/LT4R-LYBK] (last visited Aug. 14, 2019). According to the U.S. Cyber Command, “adversaries operate continuously below the threshold of armed conflict to weaken our institutions and gain strategic advantages.” U.S. CYBER COMMAND, U.S. DEPT OF DEFENSE, ACHIEVE AND MAINTAIN CYBERSPACE SUPERIORITY: COMMAND VISION FOR US CYBER COMMAND 3 (Apr. 2018), https://www.cybercom.mil/About/Mission-and-Vision/ [https://perma.cc/4EAP-L7N4] (last visited July 7, 2020). The Command Vision seeks persistent, global engagement against adversaries: “We sustain strategic advantage by increasing resiliency, defending forward, and continuously engaging our adversaries.” Id. at 6. In other words, DoD is pursuing cyber adversaries on a proactive global basis as a military activity. See also Robert Chesney, The 2018 DOD Cyber Strategy: Understanding “Defense Forward” in Light of the NDAA and PPD-20 Changes, LAWFARE( Sept. 25, 2018), https://www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes [https://perma.cc/A59J-XW5P] (last visited July 29, 2019) (arguing that this “leaves us with the conclusion that defense forward entails operations that are intended to have a disruptive or even destructive effect on an external network: either the adversary’s own system or, more likely, a midpoint system in a third country that the adversary has employed or is planning to employ for a hostile action”).
cyber operations, and covert operations. This problem, not clarified by the 2019 NDAA, cannot be overemphasized; many cyber activities elude characterization under the definitions that traditionally applied to physical activities.  

Initially, Congress granted the DoD broad authority to conduct activity for a broad range of purposes, as the statute’s inclusion of DoD terminology such as “preparation of the environment” and “information operations” was vague and undefined in other statutes. In turn, this raises issues about how certain cyber activities should be viewed under domestic and international law, and raises a risk that a collection or an exploitation activity could be construed by an adversary as a threat of force or even a use of force in violation of the U.N. Charter.

In clandestine collection, traditional espionage involving a foreign agent (e.g., a spy), can occur through computer networks to collect foreign intelligence information regarding an adversary’s computer, computer systems, or information or communications systems, as well as networks that may facilitate future operations. However, the term “clandestine” used in the 2019 NDAA is not defined by law. Such cyber collection may be even more effective than traditional espionage activity; remote cyber operations can extract large volumes


29 This term is used by the DoD as an “umbrella term for operations and activities conducted by selectively trained special operations forces to develop an environment for potential future special operations.” U.S. DEP’T OF DEFENSE, DOD DICTIONARY OF MILITARY AND ASSOCIATED TERMS 175 (June 2019). See also U.S. DEP’T OF DEFENSE, JOINT PUBL’N 3-05, SPECIAL OPERATIONS II-5 (July 2014).

(Explaining that operational preparation of the environment activities include are “intended to prepare for near-term [direct action],” and may include, but are not limited to “close-target reconnaissance; tagging, tracking, and locating (TTL); reception, staging, onward movement, and integration (RSOI) of forces; infrastructure development; and terminal guidance.”). In other words, the DoD sees the “preparation of the environment” as a range of activities in preparation for the near-term use of force against an identified adversary. In a cyber context, this preparation could involve a range of cyber activities (e.g., the insertion of a “trap door” or “malware” into a foreign system) intended to facilitate subsequent, but not necessarily already approved outside the DoD, offensive operations.

30 This term is defined by the DoD as the “integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.” U.S. DEP’T OF DEFENSE, DOD DICTIONARY OF MILITARY AND ASSOCIATED TERMS 108 (June 2019). See generally U.S. DEP’T OF DEFENSE, JOINT PUBLICATION 3-13, INFORMATION OPERATIONS (Nov. 2014).

31 See, e.g., 10 U.S.C § 394(c) (2018) (referring to “clandestine activities or operations”). Still, the DOD DICTIONARY OF MILITARY AND ASSOCIATED TERM defines “clandestine” as an “operation sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment.” Id. at 37. By contrast, the Dictionary then defines a covert “operation that is so planned and executed as to conceal the identity of or permit plausible denial by the sponsor.” Id. at 55.
of data without the assistance of an recruited spy or his American case officer. While there is no general prohibition under international law regarding espionage in peacetime, a collection activity could constitute a violation of foreign domestic (criminal) law or, more generally, incur state responsibility as an internationally wrongful act in violation of customary international law. The term “cyber exploitation,” as used in this article, refers to network penetrations that enable future operations, such as the insertion of a trap door or malware that performs certain command functions. Cyber exploitation can

35 A “trap door,” also known as a back door, is a secret method created by a programmer for gaining subsequent access to a computer application, a system or an on-line service. A programmer can create a trap door for either legitimate (e.g., troubleshooting or repair) or illegitimate (e.g., hacking) reasons. David Dunning, What Is a Computer Trapdoor?, TECHWALLA, https://www.techwalla.com/articles/what-is-a-computer-trapdoor (last visited July 24, 2019).
36 “Malware” is a general term that describes malicious software such as bots, viruses and worms. TALLINN MANUAL, supra note 11, at 566.
37 According to the National Research Council, cyber-attack and cyber exploitation require a “vulnerability, access to that vulnerability, and a payload to be executed – the only difference is in the payload to be executed.” Nat’l Res. Council, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities (William A. Owens et al. eds., 2009). According to one report, computer network exploitation involves data extrapolation or manipulation, while computer network attack is the military
involve intelligence collection as well as preparations a cyber-attacks. A cyber-attack “refers to deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks.”  Consequently, a cyber exploitation against foreign critical infrastructure, such as a missile development program or nuclear command and control systems, could be perceived by an adversary as escalatory in a crisis situation.

Cyber-attacks may range from an unacknowledged DDoS attack with temporary effects, such as the recent service outage in North Korea, to a broader, more destructive conduct as in the Stuxnet attack perpetrated against Iranian nuclear facilities. Cyber-attacks have the potential to constitute a use of force, a threat of force, or an armed attack under international law, depending on the circumstances of the attack. For instance, experts disagree on whether the 2010 Stuxnet attack was both a use of force and also an armed attack under the U.N. Charter. This lends itself to considerable ambiguity in parlance for offensive operations; the report indicates that the concepts are closely related and sometimes indistinguishable. CATHERINE A. THEOHARY & ANNE I. HARRINGTON, CONG. RES. SERV., R43848, CYBER OPERATIONS IN DOD POLICY AND PLANS: ISSUES FOR CONGRESS 16 (2015). Neither the current JP 3-12, CYBERSPACE OPERATIONS, June 8, 2018, nor JP 3-13, INFORMATION OPERATIONS, Nov. 20, 2014, defines the term “computer network exploitation” even though both publications use it.

38 Nat’l Research Council, supra note 37, at 21. 1979 Protocol I, art. 49 (1), defines “attacks” as “means of violence against the adversary, whether in offense or in its defense.” Under the TALLINN MANUAL, supra note 11, Rule 92, a “cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.”


42 TALLINN MANUAL, supra note 11, Rule 69 provides that a “cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.” Id. at 330. See also MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 45-67 (2014).

43 Roscini, supra note 42, at 67-69.

44 Id. at 70-77.


46 Id. art. 51.

the statutory meaning of the term “military activities in cyberspace short of hostilities ….” 48 Presumably, such cyber-attacks could qualify as “sensitive military cyber operations” and come under the closer — albeit ex post facto — reporting requirements under 10 U.S. Code § 395, 49 although the statute leaves considerable room for interpretation because it does not distinguish sensitive military operations from covert actions.

Next, there are new questions about the nature of presidential and congressional oversight. The new statutory authorization allows for a range of offensive cyberspace operations that could be properly characterized as a covert action, but absent executive oversight required, such as is required for a presidential finding and Memorandum of Notification to the Congressional intelligence committees. 50 The new language creates an important change in congressional reporting requirements; the statute provides that “[the Secretary of Defense] shall brief the congressional defense committees about any military activities or operations in cyberspace, including clandestine military activities or operations in cyberspace, occurring during the previous quarter during the quarterly briefing required by section 484 of this title.” 51 In other words, the DoD and U.S. CYBERCOM can conduct a broader range of offensive cyberspace operations, some which may be construed by an adversary as a hostile or wrongful act in violation of international law, but the Secretary of Defense is no longer constrained by the requirement of a presidential finding, 52 prior or contemporaneous reporting to Congress, 53 or even reporting to the senior

48 10 U.S.C § 394(b).
49 10 U.S.C § 395(a) requires that “Secretary of Defense shall promptly submit to the congressional defense committees notice in writing of any sensitive military cyber operation conducted under this title no later than 48 hours following such operation.” Section 395(c)(1) then defines the term “sensitive military cyber operation” as an action that:
(A) is carried out by the armed forces of the United States; and
(B) is intended to cause cyber effects outside a geographic location—
(i) where the armed forces of the United States are involved in hostilities (as that term is used in section 1543 of title 50, United States Code); or
(ii) with respect to which hostilities have been declared by the United States.” Id.
The statute does, however, state that the notification requirement does not apply “to a covert action (as that term is defined in section 503 of the National Security Act of 1947 (50 U.S.C. 3093)).” 10 U.S.C § 395 (d)(2) (2018)
51 10 U.S.C. § 394(d).
52 50 U.S.C. § 3093(a)(1)(2014). Kuyers argues that:
“the true power behind the presidential finding requirement is that it imposes an internal review of covert operations on the Executive branch and makes it more difficult for the President to deny knowledge of an operation if it ends in disaster.”
53 50 U.S.C. § 3093(a)(2) provides that: “Except as permitted by paragraph (1), a finding may not authorize or sanction a covert action, or any aspect of any such action, which already has occurred.”
congressional leadership. In one sense, the 2019 NDAA has a broader requirement for congressional reporting than the covert action statute; the 2019 NDAA does not include a provision that could be used to limit congressional reporting on sensitive military cyber operations to the “gang of eight.”

The traditional controls on uses of force, whether involving covert actions or armed conflict, exist to ensure executive and congressional oversight, as well as political accountability through elections, in the conduct of U.S. foreign policy. There is a distinct difference between purely defensive actions, which are either responses against an on-going attack or the preparation of capabilities for prospective conflict, and offensive operations that could initiate or escalate a crisis. On one hand, it is true that the DoD experienced difficulties in obtaining mission approval within the executive branch for peacetime cyber operations that involved conduct beyond intelligence collection or a response to an on-going attack. That there has been disagreement over the propriety of certain activities is no doubt a reflection on the unique nature of certain cyber activities and the perhaps unknowable consequences that may result from them. Indeed, the United States has periodically faced intelligence crises resulting from ill-advised operations, such as the 1985-87 Iran-Contra affairs, that had been decided within a limited group of senior officials, without the benefit of interagency review and debate. Thus, the short-circuited approval process encapsulated in the 2019 NDAA—albeit to intended to facilitate timely responses to on-going attacks—is not necessarily a positive development.

However, strong presidential control and prior congressional notification perform an important function: they ensure that the United States uses unacknowledged force only in pursuit of “identifiable foreign policy objectives of the United States and is important to the national security of the United States.” The need to inhibit unintended escalation with a foreign adversary mandates high quality intelligence to minimize the risk of misattribution and collateral damage, as well as tight political control. Now, however, the DoD can conduct a range of offensive cyberspace operations (i.e., “defend forward”

---

54 50 U.S.C. § 3093(c)(2) provides that:

“If the President determines that it is essential to limit access to the finding to meet extraordinary circumstances affecting vital interests of the United States, the finding may be reported to the chairmen and ranking minority members of the congressional intelligence committees, the Speaker and minority leader of the House of Representatives, the majority and minority leaders of the Senate, and such other member or members of the congressional leadership as may be included by the President.”

Thus, the “gang of eight” includes the leaders of each of the two parties from both the Senate and House of Representatives, and the chairs and ranking minority members of both the Senate and House Committees for Intelligence.


through “persistent engagement”\textsuperscript{58} independent of any explicit finding to that effect. The DoD has the authority to conduct a broad range of activities that it may consider “short of hostilities,”\textsuperscript{59} but ones that an adversary may consider as a hostile or internationally wrongful act.

It is, therefore, important to consider how offensive cyberspace operations are regulated under domestic and international law—with special emphasis on how clandestine, sensitive, and covert cyber actions present special challenges for policymakers and practitioners alike. Arguably, the 2019 NDAA has clarified the relatively innocuous notion that military intelligence collection activities—whether styled as clandestine, preparation of the environment, or information operations—are exempted from the covert action statute as a TMA.\textsuperscript{60} Still, the 2019 NDAA fails to distinguish between cyber collection activities, sensitive military cyber operations, and cyber covert actions.\textsuperscript{61} In effect, the U.S. CYBERCOM is now preauthorized to commit internationally wrongful acts with an attendant risk to U.S. foreign policy objectives and national security interests, without prior interagency coordination or presidential approval, provided that such acts are “short of hostilities,” according to the DoD.\textsuperscript{62} This lack of clarity is problematic with the ambiguity that is inherent in characterizing in cyber activities. In other words, offensive cyberspace operations, not intended by the United States as a hostile act, could be readily viewed as such by a foreign adversary and could, therefore, lead to unintended and unwanted consequences.

Effective regulation under this scheme, involving both presidential control and congressional oversight over military cyber operations, would help ensure that such actions serve as a viable foreign policy tool that advances U.S. national interests without the unnecessary risk of crisis escalation. First, the change in the characterization of clandestine military cyber operations as a “traditional military activity” is undoubtedly a useful one that reduces the need for unnecessary interagency coordination.\textsuperscript{63} Nonetheless, when such activities are conducted “in areas in which hostilities are not occurring,”\textsuperscript{64} the DoD and the U.S. CYBERCOM should be obligated to inform the State Department, as well as the Director of National Intelligence, in advance of the proposed operation. In other words, the uncoordinated conduct of military cyber operations abroad risks conflict with U.S. relations with foreign countries and with other foreign intelligence collection activities.

Second, the statute should be amended to clarify the terminology involving the “preparation of the environment, information operations, force protection,

\textsuperscript{58} U.S. DEPARTMENT OF DEFENSE, supra note 20, at 1. \textit{See also} U.S. CYBER COMMAND, supra note 26, at 6.
\textsuperscript{59} 10 U.S.C. § 394(b).
\textsuperscript{60} 10 U.S.C. § 394(c).
\textsuperscript{61} See 10 U.S.C. § 394(a).
\textsuperscript{62} \textit{See id.}
\textsuperscript{63} \textit{Id.}
\textsuperscript{64} 10 U.S.C. § 394(b).
and deterrence of hostilities, or counter-terrorism operations involving the
Armed Forces of the United States.\textsuperscript{65} This language, undefined in the statute, is
vague and overbroad; it not only authorizes a wide range of defensive activities,
but also many offensive activities, from the insertion of “malware” to facilitate
possible future operation to an outright attack (i.e., otherwise indistinguishable
from a covert action). On one hand, in the face of an on-going cyber-attack
against the United States, the DoD should have the full legal authority to not
only defend its own systems, but also to use timely and proportionate
countermeasures against that adversary. Thus, the DoD should have the legal
authority to conduct such defensive operations without the need for interagency
coordination or even prior presidential approval. And, as applied to defensive
activities, to include proportionate countermeasures, the post-operational
briefings to the congressional defense committees for “any military activities or
operations in cyberspace”\textsuperscript{66} or a “sensitive military cyber operation”\textsuperscript{67} are
entirely appropriate. On the other hand, planned, offensive “military activities
or operations in cyberspace short of hostilities … or in areas in which hostilities
are not occurring”\textsuperscript{68} should be subject to interagency coordination, presidential
approval, and notification to Congress in the same manner as a covert action.\textsuperscript{69}

Finally, the statute should be clarified with respect to congressional reporting.
Thus, conduct of military cyber operations—especially ones that may otherwise
be indistinguishable from covert actions—should be reportable to both the
congressional defense and intelligence committees. On a domestic level,
offensive cyberspace operations raise a risk of complicating foreign relations
and the unnecessarily escalation of a foreign crisis. On an international level,
offensive cyberspace operations raise a risk of an internationally wrongful act,
incurring state responsibility before an international court, as well as a possible
violation of the U.N. Charter.

II. CYBER USES OF FORCE UNDER U.S. LAW

In general terms, constitutional and statutory law impose significant process
and substantive constraints on the use of covert action as an instrument of U.S.
foreign policy. Historically, both Congress and the American people have
recognized the utility of certain intelligence activities while at the same time
voicing concerns about their ends, ways and means.\textsuperscript{70} At the same time,

\textsuperscript{65} Id.
\textsuperscript{66} 10 U.S.C § 394(d) (providing for reporting to the congressional defense committees on
a quarterly basis).
\textsuperscript{67} 10 U.S.C § 395(a) (providing for reporting to the congressional defense committees “not
later than 48 hours after such operation.”).
\textsuperscript{68} 10 U.S.C § 394(d).
\textsuperscript{69} 50 U.S.C. § 3093.
\textsuperscript{70} See, for example, LOCH K. JOHNSON, A SEASON OF INQUIRY REVISITED: THE CHURCH
COMMITTEE CONFRONTS AMERICA’S SPY AGENCIES 42-44 (2015) (expressing congressional
outrage that the CIA had had been involved in assassination plots). Indeed, the concerns
Congress has imposed higher standards on the conduct of covert actions than on either traditional military or law enforcement activities, no doubt due to the unique foreign policy implications, including the risk of war or damage to diplomatic relations, of such actions. All too often, intelligence practitioners, national security lawyers, Members of Congress and journalists use terminology, such as “clandestine operations,” “covert actions,” “traditional military” or “law enforcement activities,” or “operational preparation of the environment,” in an inexact manner, perhaps deliberately so, causing some confusion in properly characterizing such operations and activities for oversight purposes. Still, covert cyber action promises great benefits as a tool of U.S. foreign policy, provided that it is subject to a range of legal restrictions with congressional oversight.

A. Public Policy Concerns

The 1975 Report of the Senate Select Committee on Intelligence (SSCI) likely provides the seminal review on U.S. intelligence activities, including a range of sensitive activities. Covert actions have had a major impact on U.S. foreign policy over the past few decades, either furthering or complicating the pursuit of significant national interests. In some cases, such the attempted assassination of a foreign political leader or support of a coup that overthrows a government, the consequences can be long-term and serious. As an example, the United States’ 1953 support for the coup that toppled the elected Iranian government of Mohammad Mosaddegh and brought the Shah back to power still colors U.S.-Iranian relations. In other cases, covert actions such as the Iran-Contra Affairs in the mid-1980’s undoubtedly violated U.S. law. As a result, the U.S. Congress and the American people expect a certain level of presidential direction and control, with notification to the congressional oversight committees. Still, the President’s authority to manage intelligence activities and maintain secrecy gives him great discretion subject to limited congressional

expressed by Senator Frank Church (D-ID) regarding plots against a foreign head of state, not at war with the United States, are readily understandable. Such action could be construed as an “act of war” by the United States, as well as a violation of the U.N. Charter, art. 2(4).

53 See generally Kuyers, supra note 52 (seeking to provide a degree of clarity regarding the use of terminology in the Title 10/50 debate).
54 See generally Stephen Kinzer, All the Shah’s Men: An American Coup and the Roots of Middle East Terror (2003); Mark Bowden, Guests of the Ayatollahs (2006); and David Crist, The Twilight War: The Secret History of America’s Thirty-Year Conflict with Iran (2012).
restrictions. In a certain sense, covert action is not—strictly speaking—an intelligence activity, but is rather a foreign policy tool used by the President. Like any tool, it can be used for great positive effect or it can inflict significant damage.

B. Constitutional Law

The U.S. Constitution provides the starting point for any use of force analysis under domestic law. While Congress retains the power to “declare War,” the President has broad constitutional and statutory authorities when it comes to national security. Generally, the President and the Secretary of Defense have wide-ranging authority to conduct traditional military activities under Title 10, while Title 50 governs foreign intelligence activity including covert action.

The important point here is that the Secretary of Defense has intelligence and operational authorities under Title 10. Moreover, the Executive branch has promulgated at least five presidential directives and executive orders on cyber security issues, although none appears to have addressed covert cyber action.

Still, there are open issues in several statutes that, combined with executive secrecy and limitations in congressional oversight, create a risk for policy failure and unwarranted violations of international law.

Initially, the Constitution gives both the Executive branch and Congress powers regarding “War” and over the uses of force. Article I gives Congress the power to “declare War,” “raise and support Armies,” to “make Rules for the Government and Regulation of the land and naval Forces,” and to “make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers ….” Indeed, Article I undoubtedly gives Congress expansive powers that can regulate the means and methods of covert action in great detail.

77 U.S. CONST. art. I, § 8, cl 11.
78 U.S. CONST. art. II, § 2, cl 1 (the Commander-in-Chief clause).
79 Robert Chesney, Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate, 5J. Nat’l Sec. L. & Pol’y 539, 539 (2012). He argues that: “the most striking features of the post-9/11 era has been the convergence of military and intelligence operations. Nothing illustrates the trend better than the CIA’s emergence as a veritable combatant command in the conflict with al Qaeda, though it manifests as well through the expansion of clandestine special forces activities, joint CIA-special forces operations, and cyber activities that defy conventional categorization.” Id. at abstract. He believes that the legal authorities in this area have not been well understood and that has caused some confusion for lawyers and policy makers.
81 U.S. CONST. art. I, § 8, cl 11.
82 U.S. CONST. art. I, § 8, cl 12.
84 U.S. CONST. art. I, § 8, cl 18.
even if not explicitly mentioned in the text. Article II vests the President with the “executive power,”\textsuperscript{85} which confers upon him powers as the Commander-in-Chief of the armed forces.\textsuperscript{86} While this grant of authority provides the President with broad authority to use force for either offensive or defensive purposes, it is subject to a range of congressional restrictions.\textsuperscript{87} There are several ways that Congress can limit the President’s domestic authority, including action through the “power of the purse,”\textsuperscript{88} if the President pursues an independent course. Nonetheless, in cases where the President directs covert action pursuant to the statutory authorities enacted by Congress, “his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate.”\textsuperscript{89} The President’s use of statutory process also places covert actions squarely under the lamp of congressional oversight, helping to ensure that such actions are lawfully conducted and advance U.S. foreign policy interests.

The first possible limitation on the President’s authority to use covert forces abroad involves the “declare War” clause.\textsuperscript{90} This apparent grant of authority to

\textsuperscript{85} U.S. Const. art. II, § 1, cl. 1. Some scholars note a difference between Article I, §1 in which Congress receives “All legislative Powers herein granted” and Article II, § 1 that says the “executive Power shall be vested in a President of the United States of America.” By one reading, the Congress has received a closed list of powers, while the President has open-ended powers. This leads to a question about the possible expansive nature of the President’s authorities especially as it relates to national security and foreign affairs issues. Compare Saikrishna B. Prakash & Michael D. Ramsey, The Executive Power Over Foreign Affairs, 111 Yale L.J. 231, 234, 266, 355 (2001) (arguing for a broad view of the executive power), and Curtis A. Bradley & Martin S. Flaherty, Executive Power Essentialism and Foreign Affairs, 102 Mich. L. Rev. 545, 551 (2004) (taking a more conservative view of the executive power).

\textsuperscript{86} U.S. Const. art. II, § 2, cl 1.

\textsuperscript{87} David J. Barron & Martin S. Lederman, The Commander in Chief at the Lowest Ebb – Framing the Problem, Doctrine, and Original Understanding, 121 Harv. L. Rev. 689, 745 (2008); David J. Barron & Martin S. Lederman, The Commander in Chief at the Lowest Ebb – A Constitutional History, 121 Harv. L. Rev. 941, 944-47 (2008). In this two-part article, Barron and Lederman discuss the usages of the Commander-in-Chief clause, to include how that authority has been understood by the President and Congress throughout U.S. history. Contrary to many who believe that the Congress has often acquiesced to uses of force by the President, Barron and Lederman argue that the Commander-in-Chief often operates in a legal environment subject to a range of congressionally imposed limitations save for limited exceptions in the President’s superintendence role. Indeed, the lowest ebb reference stems from Justice Robert Jackson’s famous concurring opinion in Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952) (Jackson, J., concurring). In other words, in cases:

“When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter.” Id. at 637.

\textsuperscript{88} U.S. Const. art. I, § 8, cl 12.

\textsuperscript{89} Youngstown, 343 U.S. at 635.

\textsuperscript{90} U.S. Const. art. I, § 8, cl 11.
the Congress to decide when and, to some extent, where to use military forces abroad has imposed limited restraint on the President’s actions under his Commander-in-Chief authority.\textsuperscript{91} The 2001 Authorization for Use of Military Force (AUMF),\textsuperscript{92} passed by Congress in the wake of the 9/11 attacks against the United States, could be construed as a Declaration of War, especially if applied to either al Qaeda, one of its co-belligerent organizations, or a state sponsor of any such terror group. Here, the President could use the AUMF as his domestic legal authority to order a covert cyber-attack against al Qaeda or one of its media outlets. Nonetheless, the President is precluded by statute from conducting operations which are “intended to influence United States political processes, public opinion, or media.”\textsuperscript{93} Hence, the President might be constrained from ordering a cyber-attack that involves the use of propaganda or disinformation against a media outlet, but would not necessarily be constrained in an attack that results in an impairment or denial of services.

A second possible limitation on the President’s authority to use covert forces abroad involves the 1973 War Powers Resolution.\textsuperscript{94} The WPR focuses on the deployment of troops to a foreign conflict area and imposes an obligation upon

\textsuperscript{91} According to the Congressional Research Service, the United States has used force hundreds of times during the period 1798-2015, but there have been only 11 instances of a congressionally “declared War.” BARBARA SALAZAR TORREON, CONG. RESEARCH SERV., R42738, INSTANCES OF USE OF UNITED STATES ARMED FORCES ABROAD, 1798-2015 1 (2015).

\textsuperscript{92} Authorization for Use of Military Force Against September 11 Terrorists, Pub. L. No. 107-40, 115 Stat. 224 (2001) (codified at 50 U.S.C. § 1541 (2006)). The AUMF provides that “the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.”

This sweeping authorization has a wide ranging geographic and temporal reach; it could be construed to authorize covert military actions on a global basis. See also Jennifer C. Daskal, The Geography of the Battlefield: A Framework for Detention and Targeting Outside the ‘Hot’ Conflict Zone, 161 U. PA. L. REV. 1165, 1176, 1180 (2013).


\textsuperscript{94} The War Powers Resolution, 50 U.S.C. §§ 1541–1548 (1973). Numerous commentators have questioned the constitutionality of the WPR, as well as its non-application to limited uses of military force by the President such as the 1986 raid on Libya in response to the earlier bombing attack on U.S. military personnel at a Berlin nightclub, the 1998 cruise missile strikes against al Qaeda camps in Afghanistan, the 2011 no-fly zone that was imposed on Libya under U.N. Security Council Resolution 1973, or a special operations mission to rescue American citizens. Compare Stephen L. Carter, The Constitutionality of the War Powers Resolution, 701 VA. L. R. 101, 101 (1984) (arguing that the War Powers Resolution is not constitutional as an exercise of the war power; rather, it is constitutional in that it defines the war power), and Robert L. Turner, The War Powers Resolution: Unconstitutional, Unnecessary, and Unhelpful, 17 LOY. L.A. L. REV. 683, 683 (1984) (he finds at least four constitutional problems within the three sections of the resolution).
the President to withdraw the troops absent congressional approval within 60-90 days.\textsuperscript{95} Notably, without a specific congressional prohibition, no congressional authority or advance notification is required for the “movement” of military forces or a wide range of activities that could be made in preparation for active operations.\textsuperscript{96} Arguably, some other limited presidential actions might be construed as acts short of “war,” if they are limited in time or purpose, and thereby evade the strictures of the WPR. Thus, one could argue that a short-term “law enforcement operation,”\textsuperscript{97} not directed at the sovereignty or independence of another state, does not implicate the WPR. This statute is, therefore, unlikely to impose a practical limitation on the use of offensive cyberspace operations: a focused, digital attack can be conducted with military “forces” that never leave the continental United States, and any such operation could be completed within days, if not hours.

\textsuperscript{95} 50 U.S.C. § 1543(a) requires that the President submit reports to Congress in certain circumstances in which the U.S. Armed Forces have been introduced into hostilities in the absence of a declaration of war, and that:

“Within sixty calendar days after a report is submitted or is required to be submitted pursuant to section 1543(a)(1) of this title, whichever is earlier, the President shall terminate any use of United States Armed Forces with respect to which such report was submitted (or required to be submitted), unless the Congress (1) has declared war or has enacted a specific authorization for such use of United States Armed Forces, (2) has extended by law such sixty-day period, or (3) is physically unable to meet as a result of an armed attack upon the United States.” \textit{Id.} at § 1544(b).

\textsuperscript{96} Congress has imposed restrictions on the overall numbers of personnel that may be deployed to a country, such as El Salvador during the 1980’s, or on the use of appropriated funds for certain purposes, such as the support to Nicaraguan’s Contras during the 1980’s. \textit{See, e.g.}, El Salvador Military Aid Reduction and Restrictions Act of 1990, S.2954, 101st Cong. § 5 (1989-1990) (limiting the amount of military assistance to El Salvador for Fiscal Year 1991 under certain conditions), or the earlier Boland Amendments, Pub. L. No. 97-377, 96 Stat. 1865 (1982) (prohibiting American assistance in training, equipping, or advising the Contras).

\textsuperscript{97} One example of this might be the 1976 Israeli raid at Entebbe International Airport to rescue hostages held by aircraft hijackers. William Stevenson, \textit{90 MINUTES AT ENTEBBE: THE FULL STORY OF THE SPECTACULAR ISRAELI COUNTERTERRORISM STRIKE AND THE DARING RESCUE OF 103 HOSTAGES} (2015) (this interesting book also contains verbatim excerpts from the debate in the U.N. Security Council after a subsequent complaint was lodged by the Government of Uganda; the Israeli response, with detailed facts and legal argument, made by its ambassador provides clear and convincing evidence of Ugandan state support to the terrorists). The Israeli intervention could probably be best characterized as a proportionate countermeasure taken in response to an antecedent internationally wrongful act and consistent with the Articles on Responsibility of States for Internationally Wrongful Acts (2001) prepared by the International Law Commission. G.A. Res. 56/83 (XXII), at 6 (Jan. 28, 2002). In a like manner, a cyber operation to recover stolen intellectual property from a non-state actor could be construed as a “law enforcement operation” under domestic law and a proportionate countermeasure under international law.
C. Statutory Law

The U.S. Congress has passed two important statutes that bear on the conduct of intelligence operations abroad, particularly in cases where the congressional “war powers” are not implicated. The covert action statute, 50 U.S.C. § 3093, is designed to ensure that covert actions remain a limited yet focused tool of U.S. foreign policy.98 This statute imposes process and substantive requirements on the President, especially with regard to oversight by the congressional intelligence committees.99 The second statute, 12 U.S.C. § 3927, addressing the Chief of Mission authority of a U.S. ambassador to a foreign country, is designed to ensure the effective direction and control of all Executive branch activities in a foreign country; this statute serves as a useful tool for Executive oversight.100 While U.S. government employees serving overseas undoubtedly recognize and respect this authority as a general practice, it has sometimes been ignored, creating some risk to U.S. national interests.101

The covert action statute, 50 U.S.C. § 3093, establishes requirements for a written finding by the President and with a memorandum of notification to the intelligence oversight committees.102 The President must make a written finding that the action is “necessary to support identifiable foreign policy objectives of the United States and is important to the national security of the United States.”103 Each finding must specify each “department, agency, or entity of the United States Government authorized to fund or otherwise participate in any significant way in such action.”104 Moreover, the Director of National

---

99 Id.
104 50 U.S.C. § 3093(a)(3). According to John Rizzo, former Acting General Counsel at the CIA, he “could not recall a single instance in his many years of dealing with this issue in which an agency other than the CIA sought and received the required written finding to conduct a covert action – even the U.S. military.” See Matthew Dahl, Event Summary: The
Intelligence is obligated to keep the “congressional intelligence committees fully and currently informed of all covert actions”\(^\text{105}\) and can limit reporting to the “gang of eight” in the case of sensitive military cyber operations.\(^\text{106}\) A covert action must be distinguished from a secret military intelligence activity. Thus, the statute sets out specific congressional reporting requirements for a covert action and indicates that there is no explicit requirement for control by the Central Intelligence Agency (CIA) over such an action.\(^\text{107}\) However, the Secretary of Defense has a more general obligation to keep “the congressional intelligence committees fully and currently informed of all intelligence activities, other than a covert action (as defined in section 503(e)), … including significant anticipated intelligence activity and any significant intelligence failure ….”\(^\text{108}\) In other words, the Secretary is neither obligated to review a presidential finding nor submit a memorandum of notification to Congress in advance of a secret military intelligence activity, yet the Secretary cannot limit his reporting to the “gang of eight.” This raises an important issue: do the congressional intelligence committees have greater or lesser oversight over offensive cyberspace operations if conducted as a covert action or if conducted as a “traditional military activity”\(^\text{111}\)?

The statute defines “covert action” as “an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged public ….”\(^\text{109}\) Finally, the statute excludes from its ambit certain intelligence collection, as well as traditional military, diplomatic and law enforcement activities.\(^\text{110}\) This statutory definition and a set of exceptions creates significant space for low profile “military” cyber operations to escape congressional oversight, including coordination with either the CIA or U.S. ambassadors serving overseas. This practice risks violations of international law, with considerable risk to U.S. foreign policy interests.

The distinction between covert action and “traditional military activities” (TMA)\(^\text{111}\) can be analyzed in terms of the need for an unacknowledged role by

\(^{105}\) 50 U.S.C. § 3093 (b).

\(^{106}\) 50 U.S.C. § 3093 (c)(2).

\(^{107}\) 50 U.S.C. § 3093(a)(3) provides only that:

“The any employee, contractor, or contract agent of a department, agency, or entity of the United States Government other than the Central Intelligence Agency directed to participate in any way in a covert action shall be subject either to the policies and regulations of the Central Intelligence Agency, or to written policies or regulations adopted by such department, agency, or entity, to govern such participation.”


\(^{109}\) U.S.C. § 3093(e).

\(^{110}\) Id.

\(^{111}\) 50 U.S.C. § 3093(e)(2).
the United States, the nature and complexity of the operation, and the risk to U.S. foreign policy interests—which all require the need for coordination with U.S. ambassadors and the congressional oversight committees. First turning to TMA, TMA typically involves military personnel under the direction and control of a U.S. military commander, either preceding or related to ongoing hostilities, where the U.S. role in the operation is either apparent or later acknowledged publicly.\footnote{Theohary, supra note 37, at 15-16 (citing the Joint Explanatory Statement of the Committee of Conference, H.R. Rep. No. 145 (1991)). The legislative history for the covert action statute indicates that “[a]ctivities that are not under the direction and control of a military commander should not be considered as ‘traditional military activities.’” See Questions for the Record (subsequent to her confirmation hearing for the position of the CIA General Counsel), U.S. Senate, Caroline D. Krass, http://www.intelligence.senate.gov/131217/krasspost.pdf (accessed July 23, 2019) (citing the conference report on S. 2834, the Intelligence Authorization Act for Fiscal Year 1991). Still, if an operation is conducted under military command and control that raises the question of whether there is congressional authorization under either a Declaration of War, the 1973 War Powers Resolution, or an Authorization for Use of Military Force.}

Generally, uniformed military personnel conducting combat operations, if taken as prisoners of war, are entitled to the protections of the 1949 Geneva Conventions including combatant’s immunity from prosecution for what could otherwise be considered violations of foreign law; however, civilian personnel “who accompany the armed forces” do not necessarily receive the same protections.\footnote{See generally Geneva Conventions, supra note 2.}

The 2011 raid on Osama bin Laden’s compound in Abbottabad, Pakistan could be understood as a TMA, despite the Obama administration’s claim that it had been a covert operation, in the following ways.\footnote{Leon Panetta, CIA Chief Panetta: Obama Made ‘Gutsy’ Decision on Bin Laden Raid, PBS NewsHour (May 3, 2011), https://www.pbs.org/newshour/show/cia-chief-panetta-obama-made-gutsy-decision-on-bin-laden-raid (claiming that the operation had been under his “command”). See also John Rollins, CONG. RESEARCH SERV., R41809, Osama Bin Laden’s Death: Implications and Considerations 1-4 (2011).}

First, the 2011 AUMF provided the President with the domestic legal authority to conduct military operations against bin Laden and al-Qaeda.\footnote{See Authorization for Use of Military Force Against September 11 Terrorists, Pub. L. No. 107-40, 115 Stat. 224 (2001) (codified at 50 U.S.C. § 1541 (2006)) [hereinafter 2001 AUMF].} Second, although specialized intelligence support from the CIA was used, the small scale and focused operation—a typical military raid—employed uniformed personnel, under the direction and control of the U.S. Special Operations Command, carried to the scene by specialized military helicopters.\footnote{Panetta, supra note 114. While military personnel have been detailed/assigned to the CIA since 9/11 and work under the direction and control of the CIA Director, command authority generally runs from the President through the Secretary of Defense to the combatant commanders, unless “otherwise directed by the President.” 10 U.S.C. § 162(b) (Combatant commands: assigned forces; chain of command). Thus, if the circumstances warranted, the}
conducted under conditions of secrecy due to the violation of Pakistan’s sovereignty and the need for surprise, the swift announcement of its involvement by the United States demonstrates there was unlikely any intent that the operation would remain unacknowledged.\footnote{Barack Obama, Remarks by the President on Osama bin Laden (May 2, 2011), https://obamawhitehouse.archives.gov/the-press-office/2011/05/02/remarks-president-osama-bin-laden.}

By contrast, other cyber operations, which do not involve actual combat forces or require unique military expertise, might be more suitable for classification as a covert operation. Unacknowledged offensive cyberspace operations are not classic military operations because they lack the involvement of uniformed forces, which distinguish combatants from non-combatants on the battlefield and aid belligerents in their obligation to only target military objectives.\footnote{According to 1979 Protocol I, supra note 33, art. 44, “combatants are obligated to distinguish themselves from the civilian population while they are engaged in an attack, or in a military operation preparatory to an attack.” The United States recognizes the distinction principle to be customary international law. Matheson, supra note 33, at 420.} Indeed, cyber warriors conducting “military activities or operations in cyberspace short of hostilities … or in areas in which hostilities are not occurring,”\footnote{10 U.S.C. § 394(b).} are more like traditional spies who operate in secrecy and are not entitled to combatant immunity (such as the protections afforded a prisoner of war).\footnote{See 1979 Protocol I, supra note 33, art. 46; Vijay M. Padmanabhan, Cyber Warriors and the Jus in Bello, 89 INT’L L. STUD. SER. US NAVAL WAR COL., 288 n.22 (2013) (stating cyber warriors are similar to espionage).}

Despite these distinctions, offensive cyber exploitation, particularly by the DoD or the U.S. CYBERCOM, could nonetheless be claimed by the executive branch as a TMA under the new language in the 2019 NDAA.\footnote{10 U.S.C. § 394(b), amended by National Defense Authorization Act, H.R. 55 § 1632 (2018).} Consequently, such activity would not necessarily be constrained by either the process or substantive requirements of 50 U.S.C. § 3093. Moreover, the DoD can evade the congressional reporting obligations by characterizing robust activities (e.g., a

President could place the CIA Director in “command” of deployed military forces. Still, if this had been the case with the Abbottabad raid, the identity of the “commander” in Washington, DC should not be the dispositive factor in characterizing the operation as covert or not; the mission had all the hallmarks of a traditional military activity, to include the mission type (raid conducted under conditions of secrecy), using organized, uniformed forces with issued equipment, and with no intent that the operation would remain unacknowledged. In any case, the violation of Pakistani sovereignty had enormous explosive potential in terms of U.S. relations with that country; CIA contractor Raymond Davis had been released just two months earlier from a Pakistani jail after killing two local nationals in Lahore, an event that sparked an uproar with the Pakistani people. \textit{CIA Contractor Released after Pakistan Killings}, CNN, Mar. 16, 2011, http://www.cnn.com/2011/WORLD/asiapcf/03/16/pakistan.cia.charges/.
cyber exploitation involving the insertion of a program or device to facilitate a later attack) as “operational preparation of the environment,” and claim that the issue is within the jurisdiction of the Armed Services committees. This raises important concerns because a range of cyber activities could be construed by a foreign adversary as a hostile, escalatory act, committed as an act of aggression and in violation of state sovereignty.

The Foreign Service Act of 1980 outlines the Chief of Mission authority of a U.S. ambassador, who serves as the President’s representative to a foreign nation. In general, as Chief of Mission, the U.S. ambassador has

“(1) … full responsibility for the direction, coordination, and supervision of all Government executive branch employees in that country (except for employees under the command of a United States area military commander); and

(2) shall keep fully and currently informed with respect to all activities and operations of the Government in that country, and shall insure that all Government executive branch employees in that country (except for employees under the command of a United States area military commander) comply fully with all applicable directives of the chief of mission.”

122 Stephen Dycus, Congress’s Role in Cyber Warfare, 4 J. Nat’l Sec. L. & Pol’y 155, 161 (2010). See generally Robert D. Williams, (Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action, 79 Geo. Wash. L. Rev., 1162, 1192 (2011) (arguing that “because cyber exploitations and attacks bear such a high degree of similarity, intrusions intended as cyber exploitations may be interpreted by an adversary as an attack” and may have an adverse impact on U.S. foreign relations; thus, even if the primary purpose of an activity is collection, it may be appropriate to clear/approve it as a covert action).

123 Andru E. Wall, Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action, 3 Harv. Nat’l Sec. J. 85, 85 (2011). Wall argues that the Secretary of Defense, possessing both Title 10 and Title 50 authorities, is best suited to lead U.S. government operations against external cyber threats. Cyber operations conducted under military command and control, pursuant to an execute order issued by the Secretary of Defense, are military operations—not intelligence activities. He argues that the Congress has an antiquated oversight structure that should be revised.


“The principal officer in charge of a diplomatic mission of the United States or of a United States office abroad which is designated by the Secretary of State as diplomatic in nature, including any individual assigned under section 502(c) to be temporarily in charge of such a mission or office.”

Not all U.S. ambassadors serving overseas have Chief of Mission authority; generally, the Chief of Mission authority extends only to the ambassador representing the United States to the host nation. As an example, the United States may have two ambassadors serving in one foreign capital: an ambassador to the host nation would have Chief of Mission authority, but an ambassador to an international organization in that city would not.

As the President’s representative to that country, the ambassador could be expected to understand the intricacies of our relationship with that country, to include local sensitivities on various issues. The U.S. ambassador also has an important responsibility involving executive oversight because the uncoordinated executive activities in foreign country raises a substantial risk to U.S. diplomatic relations with the host nation. But, the clause stating that the Chief of Mission “shall keep fully and currently informed” does not actually impose an obligation on the area military commander to provide that information to him. This leaves room for misunderstandings and even deliberate efforts to sideline an ambassador, particularly if the offensive cyberspace operations are conducted through or against the target country and from the United States (e.g., Fort Meade, Maryland).

While this statute should not pose a problem for covert cyber actions conducted electronically through a second country against a third (target) country, it should be a consideration for any that entail a physical presence or cause damage or injury in a foreign country. Military commanders have a stronger argument for independence in comparison to the U. S. ambassador when the issue involves U.S. forces deployed to a declared (i.e., congressionally recognized) combat zone such as Afghanistan or Iraq; while military commanders should coordinate activities to the extent possible with the resident U.S. ambassador, the nature of the quintessentially military (combat) mission likely requires greater autonomy. However, in performing his assigned role as the President’s representative, an ambassador must have oversight over, or at least knowledge of, intelligence and military personnel deployed to his host country, such as the establishment of a cyber base of operations or a clandestine entry at a communications facility, even if the operations are conducted against a third party group or state actor. A covert operation—intended to remain

126 22 U.S.C. § 3927(b).
127 Such action could, however, violate the domestic law, as well the neutrality under international law, of that second country. Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land art. 2, Oct. 18, 1907, 36 Stat. 2310, 1 Bevans 654, 205 Consol. (“The territory of neutral Powers is inviolable.”); see also TALLINN MANUAL, supra note 11, Rule 151 (“The exercise of belligerent rights by cyber means in neutral territory is prohibited.”).
128 JEREMY SCAHILL, DIRTY WARS: THE WORLD IS A BATTLEFIELD 170-171 (2013). Scahill describes problems with the global operations of the U.S. Special Operations Command (SOCOM) subsequent to the 9/11 attacks. He offers examples of military deployments, that could have been either clandestine or covert, that were made to various countries and in the absence of coordination with either the CIA or the U.S. ambassador. Reportedly, the euphemistically described “military liaison elements” were tasked to prepare for later operations, sometimes known as “operational preparation of the environment,” by the U.S. Joint SOCOM. Scahill also explains that military personnel often preferred operating in such circumstances because it limited congressional oversight. This also raises questions whether the SOCOM is a geographic command within the meaning of the Foreign Service Act of 1980 and to what extent the DoD can use the AUMF as authority to use lethal force in operations.
permanently unacknowledged—requires closer oversight to avoid an adverse impact on U.S. foreign policy interests both in the target country and throughout the region. The U.S. ambassador to the target nation should be “fully and currently” informed about any collection or exploitation activities conducted through or against his host that could be perceived as a hostile act.

D. Executive Order 12333, United States Intelligence Activities

Executive Order (EO) 12333 was first signed by President Ronald Reagan in 1981 and has been reissued by successive presidents. EO 12333 expands the powers and responsibilities of the U.S. intelligence community (IC) and has helped facilitate some level of interagency coordination. In practice, the EO effectuates statutory controls over the IC, placing important restrictions on the full range of intelligence activities and operations. For present purposes, sections 1.7 (a)(4) and 2.13 impose limitations on covert actions and effectively implement the covert action statute. This and other EO’s, binding on Executive branch employees, are subject to revision at any time, as well as caveat through classified addendums, by the President.

Section 1.7 (a)(4) provides that no agency other than the CIA (or the armed forces during periods of war) may conduct covert operations “unless the President determines that another agency is more likely to achieve a particular objective.” This point reinforces the provisions of 50 U.S.C. § 3093: the DoD, as well as other federal executive departments and agencies can conduct covert operations, but such activities require affirmative approval by the President. Conceivably, there are some federal departments and agencies that might be better positioned to conduct certain covert actions. For example, the President could determine that the Federal Bureau of Investigation (FBI) or the Drug

against terror organizations not directly associated with the 9/11 attacks or al Qaeda and/or not operating in the Afghanistan/Pakistan area of responsibility. Even if such operations are legal, military-intelligence operations that are not coordinated with the U.S. country team raise significant risks to U.S. foreign policy and to other on-going government activities in the region.

132 See id.
133 See United States v. Yunis, 859 F.2d 953, 954 (D.C. Cir. 1988) (in 1987 Fawaz Yunis, a Lebanese national who was wanted on charges related to the 1985 hijacking of a Jordanian airliner while on the tarmac at Beirut International Airport, was lured to a yacht off the coast of Cyprus, for a purported drug deal, where he was arrested by FBI agents). While the covert action statute, 50 U.S.C. §3093(e)(3) excepts “traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities,” it is open for debate whether an extraterritorial operation, such as a kidnapping and extraordinary rendition of a foreign national to the United States using a “false flag”
Enforcement Administration (DEA)\textsuperscript{134} is best positioned to conduct a covert operation through a foreign law enforcement relationship, that the Department of Energy is the right department to lead an operation involving the proliferation of nuclear weapons, or that the National Security Agency (NSA)/U.S. CYBERCOM is best department mount a peacetime cyber-attack. It would be entirely appropriate for that other agency or department, which likely has less experience than the CIA in these matters, to follow the “policies and regulations of the Central Intelligence Agency” during the process of planning, obtaining approval for, and conducting such operations.\textsuperscript{135} Notably, regarding oversight, neither the covert action statute nor EO 12333 require Attorney General review, although it may occur as a matter of practice within the informal processes of the National Security Council, such as the “Lawyer’s Group,”\textsuperscript{136} or on a formal basis by the Justice Department and its Office of Legal Counsel.\textsuperscript{137}

\textsuperscript{134} See United States v. Verdugo-Urquidez, 494 U.S. 259, 262 (1990) (DEA agents coordinated activities with the Mexican police to seize a Mexican national on drug charges and search his residence before he was brought to the United States for prosecution). Reportedly, the DEA conducts many law enforcements operations in Mexico, typically in coordination with Mexican authorities, either to apprehend persons wanted for drug offenses or to undermine the drug cartels themselves. See Ginger Thompson, Top Lawmakers Call for Investigation of DEA-Led Unit in Mexico, PROPUBLICA (Feb. 27, 2018), https://www.propublica.org/article/top-lawmakers-call-for-investigation-of-dea-led-unit-in-mexico. Unlike the extraterritorial capture and arrest of a person wanted on federal criminal charges, it is harder to consider the supply of weapons by agents of the Bureau of Alcohol, Tobacco and Firearms (ATF) to rival drug cartels operating in Mexico to be a TMA. While the government might be strategically justified in conducting such operation, it should undoubtedly be treated as a covert operation for purposes of federal law – if for no other reasons than the risk of possible executive abuse and to U.S. foreign relations with Mexico. William La Jeunesse, Former DEA chief says 3 other federal agencies knew about Operation Fast and Furious, FOX NEWS (Feb. 10, 2012). http://www.foxnews.com/politics/2012/02/10/former-dea-chief-says-3-other-federal-agencies-knew-about-furious/.

\textsuperscript{135} 50 U.S.C. § 3093(a)(3).

\textsuperscript{136} Krass, supra note 112, at 8; see also Daphna Renan, The Law Presidents Make, 103 VA. L. REV. 805, 837-842 (2017) (reviewing President Barack Obama’s collaborative use of an interagency group of lawyers to decide legal questions).

\textsuperscript{137} See 50 U.S.C. § 3092(a)(2) (requiring the [Director of National Intelligence and the heads of departments to furnish the intelligence committees “any information or material concerning covert actions”); 50 U.S.C. § 3093(b)(2) (requiring the DNI and the heads of departments to furnish the intelligence committees “any information or material concerning intelligence activities, other than covert actions”).
Section 2.13 provides that no “covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media.” This limitation affects covert actions undertaken with intent to influence political processes in other country through disinformation in the cyber domain. This problem is also known as “blowback,” in that actions taken to affect an adversary’s systems or networks could also have an indirect and adverse effect on U.S. systems and networks. In a classic sense, the CIA is precluded from conducting covert operations involving the placement of propaganda in the foreign press, especially if such stories are likely to be reported in the U.S. media. This law would not, however, preclude other uses of journalists, such as using them to pass infected flash drives and other malware to people visiting areas where foreign governments restrict travel by Americans.

E. Conclusions on U.S. Law

The use of force has been a contentious topic throughout U.S. history, with the debate often split based upon partisan lines both in Congress and in the American public. The President has ample authority, under both constitutional and statutory law, to use force in a range of offensive and defensive scenarios—subject to certain process and substantive limitations. There is also ample room for abuse through the characterization of a covert activity as conduct that it is not a clandestine operation or a TMA, and by evasion of the Chief of Mission’s oversight.

Offensive cyberspace operations raise questions about whether such operations are intelligence or military activities, whether operations are under the direction and control of civilians or uniformed military officers, whether the congressional reporting is exclusively limited to the intelligence committees or also includes the Armed Services committees, and whether there is coordination with the U.S. ambassadors serving abroad. Indeed, effective oversight over covert actions, both within the Executive branch and the Congress, is necessary to avoid an adverse impact on U.S. foreign policy and important liaison relationships, while promoting operational effectiveness and mitigating a risk of abuse.

138 Exec. Ord. No. 12333, supra note 129.
141 50 U.S.C. § 3093(c)(2).
III. CYBER USES OF FORCE UNDER INTERNATIONAL LAW

U.S. policymakers and national security practitioners must consider a range of international law issues in deciding whether, where, and how to conduct an offensive cyberspace operation. Cyber actions may rise to the level of either a “use of force” or an “armed attack” under the Charter of the United Nations, which risks legal accountability either for the United States or for individual intelligence officers. However, Charter law does permit some level of coercion in international relations, provided that it falls below a certain level of severity and effect.

A. Uses of Force Under Charter Law

The concept of sovereignty is the cornerstone of the international nation-state system, and is codified in the Charter of the United Nations (the “Charter”). The Charter provides that:

“All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.”\(^\text{142}\)

The Tallinn Manual expressly recognizes this principle in regard to cyber activities, recognizing that a state may exercise prerogatives concerning cyber activities in its own territory.\(^\text{143}\) The concept of sovereignty applies to victim states of cyber-attacks as well as states through which such cyber-attacks are routed, implicating a breach of international law.\(^\text{144}\)

To evaluate a wrongful breach of sovereignty, the cyber-attack must be appropriately characterized under Charter law. While Article 2(4) of the Charter proscribes “the threat or use of force against the territorial integrity or political independence of any state,” Article 51 recognizes the right of self-defense if an “armed attack,” but not a use of force, occurs.\(^\text{145}\) Some hostile actions, such as

\(^{142}\) U.N. Charter, art. 2, ¶ 4.

\(^{143}\) Tallinn Manual, supra note 11, at 13-16. The Tallinn Manual was prepared as a collaborative effort by a group of “19 renowned international law experts” and a diverse peer review group, all acting in their own capacity; the manual can be considered as a “restatement” of treaty and customary international law as it applies to cyber operations. Compare id. at xii-xviii, with Statute of the International Court of Justice, art. 38 ¶ 1(d) (allowing the Court to decide cases using “teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law”).

\(^{144}\) See U.N. Charter, art. 2, ¶ 4.

\(^{145}\) Article 51 of the U.N. Charter provides:

“Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at
economic coercion, espionage, and some covert actions such as propaganda have been considered below the use of force threshold, while other interventions (e.g., the arming of guerrillas in a foreign country) have been considered a force of use, but not necessarily an armed attack. This right of self-defense is limited by the principles of necessity and proportionality. Absent a use of force taken in self-defense, or actions taken to restore international peace and security pursuant to an authorization from the Security Council, states would be obligated to seek a “pacific settlement” to the dispute under Chapter VI.

any time such action as it deems necessary in order to maintain or restore international peace and security.” U.N. Charter, art. 51.

Article 39 provides that the Security Council must:

determine the existence of any threat to the peace, breach of peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.” U.N. Charter, art. 39.

Thus, a nation-state has the inherent right of self-defense against covert actions undertaken in violation of its territorial integrity or political independence, but Member States also have an obligation to report that violation to the Security Council and seek redress in that forum.

W. Michael Reisman & James E. Baker, Regulating Covert Action 30 (2011) (noting that the lack of a prohibition in international law against economic coercion may act as a safety valve and may make states less likely to use military force).

Id. at 31-36.

The U.N. General Assembly has, for example, passed a 1974 resolution that defined certain acts, without regard to a declaration of war that constitute “an act of aggression”; this definition would also exclude certain acts of political and economic coercion. G.A. Res. 3314, at 144, (Dec. 14, 1974). Under this definition, a covert cyber action could constitute “an act of aggression” depending upon the nature and severity of the attack. Indeed, the International Law Commission issued a 2001 report to the U.N. General Assembly in which it affirmed certain tenets regarding state responsibility for internationally wrongful acts. This report serves as persuasive authority on the current state of customary international law; it defines a wrongful act of state as one that is attributable to a state and constitutes a breach of an international obligation. Int’l Law Comm’n, Responsibility of States for Internationally Wrongful Acts, U.N. Doc. A/56/49(Vol. I)/Corr.4, at art. 2 (2001)

Levi Grosswald, Cyberattack Attribution Matters Under Article 51 of the U.N. Charter, 36 Brook. J. Int’l L. 1151, 1156-57 (2011) (defining necessity as the requirement for self-defense because the situation could not be resolved by peaceful means and proportionality as the amount of force necessary to defeat an attack or to deter future aggression). This jus ad bellum definition of proportionality differs from the jus in bello definition in that it requires parties to refrain from launching any attack that may be expected to cause incidental injury or collateral damage that “would be excessive in relation to the concrete and direct military advantage anticipate ....” 1979 Protocol I, supra note 33, art. 57 (2)(iii). The United States recognizes the proportionality principle to be customary international law. Matheson, supra note 33.

The U.N. Charter, Article VI, provides that Members can bring disputes to the Security Council for investigation and possible resolution, or to the attention of the General Assembly. If both states consent, a case can be referred to the ICJ. Statute of the International Court of
The 1986 decision of the International Court of Justice (ICJ) in *U.S. v. Nicaragua* provides a useful analogy for the threshold between a use of force and an “armed attack” in the cyber context.\(^\text{151}\) The *Nicaragua* Court recognized that Nicaragua’s arming and training of guerrillas could constitute a “use of force” against El Salvador, but held that such actions did not arise to the level of an “armed attack” which would have justified self-defense actions under Article 51.\(^\text{152}\) The Court’s characterization of Nicaragua’s activity as a “frontier incident,”\(^\text{153}\) meaning that military actions are hostile but localized, suggests that a focused cyber-attack that causes only incidental injury to persons or collateral damage might also fall short of the threshold and constrain the victim’s remedies under international law.

The ICJ’s 2003 decision in the *Oil Platforms* case offers important points on the problems involving the characterization and attribution of unacknowledged actions under international law.\(^\text{154}\) By way of background, during the Iran-Iraq War, which took place from 1980 to 1988, both sides conducted attacks against international ships in the Persian Gulf. During the final years of the conflict, in what later became known as the Tanker War, Iran commenced attacks against many Kuwaiti and Saudi commercial vessels by aircraft, helicopters, missiles and warships. In response, the United States attacked and destroyed two Iranian oil platforms under the banner of self-defense. Although the United States attributed responsibility for the initial actions of the Tanker war to Iran,\(^\text{155}\) Iran shifted blame to Iraq and denied responsibility.\(^\text{156}\) The Court explained that, for the United States to demonstrate that it was justified in exercising the right of self-defense to attack Iranian oil platforms, it had to show that Iran was responsible for the attacks made upon it, and that the Iranian attacks were of such as nature as to qualify as “armed attack.”\(^\text{157}\) The Court also explained that the United States was required to show that its self-defense actions were necessary and proportional to the “armed attack,” and that the platforms attacked by the U.S. were a legitimate military target.\(^\text{158}\)


\(^{152}\) *Id.* at ¶ 230.

\(^{153}\) *Id.* at ¶ 195.


\(^{155}\) *Id.* at ¶ 25.

\(^{156}\) *Id.* at ¶ 23.

\(^{157}\) *Id.* at ¶ 51.

\(^{158}\) *Id.*
Judge Bruno Simma issued a separate opinion in which he offered that a hostile act, not necessarily reaching the “armed attack” threshold, could be countered with immediate countermeasures. He suggested:

“a distinction between (full-scale) self-defence (sic) within the meaning of Article 5 I against an “armed attack” within the meaning of the same Charter provision on the one hand and, on the other, the case of hostile action, for instance against individual ships, below the level of Article 51, justifying proportionate defensive measures on the part of the victim, equally short of the quality and quantity of action in self-defence (sic) expressly reserved in the United Nations Charter.”

In short, intermittent, small-scale cyber-attacks against an adversary could take advantage of the gap between a “use of force” and an “armed attack,” restricting the victim to either limited, immediate counter-measures or to taking the matter—with sufficient evidence regarding state responsibility—to the ICJ. Thus, even if a victim state would be willing to admit that significant vulnerabilities had existed in its national cyber defenses, it might well lack a promising means of redress.

The United States has rejected the view that a gap exists between “uses of force” and an armed attack. Harold Koh, the former Legal Adviser to the U.S. State Department, stated that “[t]he United States has for a long time taken the position that the inherent right of self-defense potentially applies against any illegal use of force. In our view, there is no threshold for a use of deadly force to qualify as an ‘armed attack’ that may warrant a forcible response.” Thus, under his perception, any use of force equate to an armed attack. This is a minority position among international experts and many state who acknowledge the gap between the use of force and an armed attack. The U.S. view raises important issues for cyber covert operations because it lowers the threshold for an armed attack, which broadens the scope of activities that would justify an armed response to an attack originating from the United States, such as a cyber-attack.

While some experts contend that Article 2(4) prohibits the prospective use of force in international relations, other experts believe that the ‘inherent right of self-defense’ permits the exercise of an anticipatory self-defense, which allows a nation can initiate a preemptive strike if it is faced with an immediate

---

159 Id. at ¶ 13.
160 Id. at ¶ 12.
161 Koh, supra note 17.
162 Id.
163 See id.
attack by a neighbor. The 1837 *Caroline* doctrine, long-considered the traditional rule under customary international law, has two requirements: the use of force must be necessary, meaning the threat is imminent and time does not allow for the pursuit of peaceful means of resolution, and the response must be proportionate to the threat.\textsuperscript{166} Thus, one nation could pursue a covert cyber-attack, tailored to the recognized *jus in bello* principles of necessity, distinction and proportionality, against another state as a means of preempting an imminent and illegal threat and/or averting war.

This leads to the important issue regarding the requisite extent of damage or injury necessary to constitute an international armed conflict. According to the Commentaries to the 1949 Geneva Conventions, an armed conflict includes any conflict between two states “leading to the intervention of armed forces.”\textsuperscript{167} Even if there is no formal declaration of war or a state denies the existence of war, *de facto* hostilities are sufficient.\textsuperscript{168} This is a practical approach: if a state has the means to redress a situation through law enforcement authorities, then it should do so, and suspects should have the full protections of domestic legal process. However, if a situation is serious and law enforcement authorities, including domestic courts, cannot mitigate the situation, then the dictates of international humanitarian law (IHL) (*jus in bello*) should control. This also makes sense on an intuitive level: law enforcement officers are trained to respect the civil liberties of citizens in the pursuit of admissible evidence regarding past acts, but are not trained in IHL; soldiers are trained in IHL, but should not be held to an entirely different legal standard in any entirely different threat environment.

B. Cyber Uses of Force

The offensive use of cyber force presents several issues under international law. First, how does one characterize such uses of force under Articles 2(4) and


Second, how does one attribute such uses to the responsible parties? As a practical matter, unless a cyber use of force can be characterized as a use of force and attributed to a state actor, then that problem should be addressed under international law as a law enforcement problem that could be adjudicated through domestic courts. However, attribution of a use of force or armed attack raises different potential remedial measures to include action by the U.N. Security Council under Chapters VI or VII to restore international peace and security, including a possible referral of the case to the ICJ.

Professor Michael Schmitt, a distinguished legal scholar at the U.S. Naval War College, provides an important conceptual model for characterizing covert cyber actions, distinguishing between actions that fall short of and those that cross the Article 2(4) threshold of an illegal “threat or the use of force against the territorial integrity or political independence of any state.”\(^\text{169}\) This threshold differentiates activities that are (or should be) governed by a law enforcement paradigm from those state actions that may trigger rights to self-defense under Article 51—if an “armed attack” occurs—or actions by the Security Council to preserve international peace and security.\(^\text{170}\) Professor’s Schmitt analysis offers a six-factor approach that assesses an operation’s severity, immediacy of its consequences, invasiveness, measurability (e.g., the extent to which the consequences of the operation are quantifiable), and presumptive legitimacy.\(^\text{171}\) Under this criteria, armed attacks “threaten physical injury or destruction of property,” trigger consequences with “great immediacy,” entail direct connection between the consequences and the attack, and represents a greater intrusion on a target state to a much more significant degree as compared to other forms of coercion (e.g. economic sanctions).\(^\text{172}\) This is a worthwhile approach in that cyber-attacks should be assessed primarily upon the provable effects (damage) imposed on the victim by the responsible state actor, rather than on whether the modality was kinetic or non-kinetic.

The problem of cyber source attribution involves complex technical issues (e.g., identification of the origin of the operation, the means and methods used), as well as identification of the responsible parties. Politically motivated cyber-
attacks can readily occur, and are often conducted by hackers (e.g., a criminal element), cyber “mobs” (e.g., the alleged Russian reaction to Estonia’s efforts to move a Soviet war memorial),\textsuperscript{173} or the “false flag” actions of a third party nation (e.g., a hypothetical South Korean deception operation that is designed to incite U.S. action against North Korea).\textsuperscript{174} Even when source computers and networks can be identified, the issue that still looms large whether the operation was conducted by state actors, by non-state actors acting as modern day “privateers” under government direction and control, or by independent persons. In some cases, attribution may be based upon intelligence assessments that consider the political-military context, media reporting, early disclosures in the press, and technical analysis. If a victim state cannot readily characterize the event as a law enforcement problem or an armed attack, much less identify the state sponsor behind it, then that state is constrained—in both a legal and practical sense—in responding to that event.\textsuperscript{175}

Koh, the former State Department Legal Adviser, asserted that established principles of international law apply in cyberspace, much as they do in other domains.\textsuperscript{176} Foreign state actions that target a U.S. based corporation (but not the U.S. government itself) could constitute a violation of U.S. sovereignty, which is how the U.S. perceived North Korea’s 2014 attack on Sony Pictures.\textsuperscript{177} On the other hand, an action by a U.S. corporation—not acting under government direction and control—against a foreign state would likely be a domestic criminal act and not a violation of the U.N. Charter.\textsuperscript{178} Koh maintains that if a “State exercises a sufficient degree of control over an ostensibly private person or group of persons committing an internationally wrongful act, the State assumes responsibility for the act, just as if official agents of the State had committed it.”\textsuperscript{179}


\textsuperscript{175} \textit{Id.} at 334.

\textsuperscript{176} Koh, \textit{supra} note 17.


\textsuperscript{178} Statute of the ICJ, \textit{supra} note 150, at arts. 3-4.

\textsuperscript{179} Koh, \textit{supra} note 17; see also JAMES CRAWFORD, \textit{THE INTERNATIONAL LAW COMMISSION’S ARTICLES ON STATE RESPONSIBILITY} (2002); Levi Grosswald, Cyberattack Attribution Matters Under Article 51 of the U.N. Charter, 36 Brooklyn J. of Int’l Law 1151, 1159-64 (2010) (explaining the differences between the “effective control” test in the Nicaragua decision and the “overall control” test in the \textit{Tadic} decision, citing the decision of
C. Accountability for Illegal Uses of Force

Intelligence practitioners, including modern cyber warriors, can be held liable for violations of international and foreign domestic law. Some violations of international law, especially those that constitute aggression or a war crime, may be subject to criminal prosecution before international fora such as the International Criminal Court (ICC). The Rome Statute established the ICC as an independent, permanent international court in “relationship with the United Nations system.” The ICC has subject matter jurisdiction over natural persons for four crimes: genocide, crimes against humanity, war crimes and the crime of aggression. While the United States withdrew its initial signature to the Rome Statute, 123 nations are currently parties. The high number of state participants demonstrates the Rome Statute’s emerging presence in international criminal law, with influence that cannot be discounted by the United States.

Foreign domestic courts can hear a wide range of claims against American intelligence officers based either upon a direct violation of the domestic law of a foreign state or through the exercise of universal jurisdiction. In regard to the former, when the United States conducts a covert action in a foreign country, such as with a kidnapping or a cyber-attack that causes injury or damages, a foreign court could prosecute any captured intelligence officers for violations of either its domestic or international law. Concerning universal jurisdiction,
many foreign courts have heard claims involving violations of international norms occurring outside the traditional jurisdiction of that court.\textsuperscript{186} According to Amnesty International, over 15 countries have exercised universal jurisdiction for violations of international law since the end of World War II.\textsuperscript{187} For instance, in Spain some activist judges have demonstrated a willingness to hear claims arising from the conduct of American, Israeli, and Chinese officials, although the Spanish Parliament is rethinking this practice and may tighten its jurisdiction.\textsuperscript{188}

The exercise of universal jurisdiction should cause the United States to plan and execute offensive cyberspace operations as a foreign policy tool of last resort. According to the American Law Institute:

“Universal jurisdiction is increasingly accepted for certain acts of terrorism, such as assaults on the life or physical integrity of diplomatic personnel, kidnapping, and indiscriminate assaults on people at large.”\textsuperscript{189}

Under the application of universal jurisdiction, it is certainly feasible that a covert action targeting a foreign political leader with assassination\textsuperscript{190} or involving a cyber-attack with second and third order effects on a nation’s critical infrastructure raises important concerns about the U.S. diplomatic relationship with that foreign country and highlights the need for expanded oversight over covert actions by the congressional committees (i.e., involving either the Senate Foreign Relations Committee or the House Foreign Affairs Committees) and the U.S. ambassador in Rome under his Chief of Mission authority.

\textsuperscript{186} While this practice has often been controversial and disputed, it has been occurring with greater frequency over the past ten years. \textit{Compare} Henry A. Kissinger, \textit{The Pitfalls of Universal Jurisdiction}, 80 FOREIGN AFF. 86 (2001) (the former Secretary of State notes that the universal jurisdiction has a recent vintage and is a problematic development in international law), with Kenneth Roth, \textit{The Case For Universal Jurisdiction}, 81 FOREIGN AFF. 150 (2001) (Executive Director of Human Rights Watch responding to Kissinger’s critique, especially as it related to the ICC and the exercise of universal jurisdiction by national courts, and argue[t] that the United States should embrace this concept).


\textsuperscript{189} \textit{Restatement (Third) of the Law: Foreign Relations Law} § 404 (AM. LAW INST. 1986).

\textsuperscript{190} The assassination of a foreign political leader, where an international armed conflict does not exist between the two countries, would likely constitute a violation of Article 2(4) as a use of force against the territorial integrity or political independence of the victim state. Sovereign nations have a right to select their own leaders; the elimination of a nation’s choice of leader is a direct assault on that nation’s political independence. In any case, the assassination or kidnapping of a foreign head of state would violate the Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons arts. 1-2, Dec. 14, 1973, 13 I.L.M. 41, 1035 U.N.T.S. 167.
infrastructure would be characterized as a terrorist act or indiscriminate assault on people.\textsuperscript{191}

\textbf{D. The Application of International Humanitarian Law to Cyber Operations}

There are unique problems with covert cyber warfare involving international humanitarian law that should be considered by policymakers and national security practitioners. First, there is the issue regarding the neutrality of states not party to an armed conflict.\textsuperscript{192} Unlike traditional military activities, cyber operations can pass through multiple intermediate servers and networks before reaching their intended target. Consequently, these operations may have harmful effects on the public and private cyber infrastructure of a state that is not a party to an armed conflict. Second, under the basic principles of IHL, necessity, distinction, proportionality and humanity undoubtedly apply to cyberspace operations.\textsuperscript{193} So, IHL seeks to find a balance between military necessity and humanitarian concerns in present day cyber operations.\textsuperscript{194}

In regard to neutrality, offensive cyberspace operations present a unique twist to the traditional rule regarding the rights of neutrals. The 1907 Hague Convention provides rules restricting belligerents from moving troops or ammunition across neutral territory,\textsuperscript{195} erecting a “wireless telegraphy station or other apparatus for the purpose of communicating with belligerent forces,”\textsuperscript{196} and requiring neutrals to prevent such acts from occurring.\textsuperscript{197} The duty of neutrals to prevent belligerent activity is limited by Article 8, which provides that “[a] neutral power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals.”\textsuperscript{198} The Tallinn Manual expressly affirms the applicability of IHL to cyber warfare and neutral states, such as the restriction on the exercise of cyber means against neutral


\textsuperscript{192} Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land art. 1, Oct. 18, 1907, 36 Stat. 2310, 1 Bevans 654 [hereinafter Hague Convention (V)] (“The territory of neutral Powers is inviolable.”).

\textsuperscript{193} See generally Owens, \textit{supra} note 37 (concluding the principles of the U.N. Charter and the Law of Armed Conflict, governing both \textit{jus ad bellum} and \textit{jus in bello}, apply to cyber operations). The report cites Jeffrey Smith, the former general counsel to the CIA (1995-1996), that “traditional U.S. interpretations of the laws of armed conflict … require covert action, whether or not it involves violent activities, to be conducted consistent with [law of armed conflict’s] requirements.” \textit{Id.} at 194-95.


\textsuperscript{195} Hague Convention (V), \textit{supra} note 192, at art. 2.

\textsuperscript{196} \textit{Id.} at art. 3 (a).

\textsuperscript{197} \textit{Id.} at art. 5.

\textsuperscript{198} \textit{Id.} at art. 8.
infrastructure\textsuperscript{199} and belligerent rights by cyber means in neutral territory,\textsuperscript{200} stating that the use of the “public, internationally and openly accessible network such as the Internet for military purposes does not violate the law of neutrality.”\textsuperscript{201} However, there is disagreement on the issue of the transmission of cyber weapons across neutral territory, as many believe it is prohibited under Article 8 of the Hague Convention.\textsuperscript{202} Lastly, a covert cyber action, at least to the extent that involves the transmission of a destructive package (e.g., programs designed to destroy nuclear centrifuges through the infrastructure of a non-belligerent party) would likely constitute a violation of the law of neutrality and the attacker would be liable for any damages that were caused to neutral infrastructure.

IHL recognizes four basic principles, necessity, distinction, proportionality and humanity, which govern the use of force in international and non-international armed conflict.\textsuperscript{203} First, international law mandates that there must be a “necessity” for an attack.\textsuperscript{204} This principle requires that a target have a definite military value.\textsuperscript{205} This principle is typically expanded to include the non-availability of non-forcible means and inability to respond otherwise to an imminent attack. This point has particular importance for covert cyber actions: to what extent have non-forcible means been exhausted before conducting the attack? And, does the target pose such a threat that time has been exhausted for alternative remedies? Second, the principle of distinction between combatants/military objectives and civilians/civilian objects is embodied in the 1977 Additional Protocol (AP) I, Article 48.\textsuperscript{206} In the cyber context, this takes relevance due to the number of targeted systems may be dual-use, or at least inter-connected, so that effects in one part will have deleterious consequences in other parts of the system.

Third, proportionality obligates parties to refrain from launching any attack “which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which

\textsuperscript{199} TALLINN MANUAL, \textit{supra} note 11, at 555-56.
\textsuperscript{200} \textit{Id.} at 556-58.
\textsuperscript{201} \textit{Id.} at 556-57.
\textsuperscript{202} \textit{Id.} at 557.
\textsuperscript{203} NELS MELZER, \textit{INT’L COMM. OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW} 77-78 (2009).
\textsuperscript{204} According to 1979 Protocol I, \textit{supra} note 33, art. 49(1), the term “[a]ttacks’ means acts of violence against an adversary, whether in offense or defense.” This term is further defined in a cyber context by the TALLINN MANUAL, \textit{supra} note 11, at 415.
\textsuperscript{205} HEATHER HARRISON DNNIS, \textit{CYBER WARFARE AND THE LAWS OF ARMED CONFLICT} 102 n.120 (2012) (noting that there must be a “necessity of defense, instant, overwhelming, leaving no choice of means and no moment for deliberation”).
\textsuperscript{206} 1979 Protocol I, \textit{supra} note 33, at art. 48.
would be excessive in relation to the concrete and direct military advantage anticipated."

There is a duty under customary international law to take all “feasible” precautions in an attack to avoid incidental injury and collateral damages. This obligation is reinforced by Article 57(3), which provides that:

“[w]hen a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected shall be that the attack on which may be expected to cause the least danger to civilian lives and to civilian objects.”

The principle on humanity, embodied in customary law and codified in treaty, provides that all persons are obligated to show respect and care for all, even their sworn enemies. The 1966 International Covenant on Civil and Political Rights, ratified by 169 countries, further recognizes that all persons have inherent dignity and inalienable rights. While attackers are obligated to observe this principle during mission planning and execution, it is unlikely to impose any specific constraints on operations because of the difficulty in defining its meaning in any given context. Thus, the principle of humanity supports the use of focused cyber-attacks that minimize collateral damage and incidental injury, at least as opposed to the kinetic alternatives.

In a practical sense, a nation state considering whether and how to conduct an attack has heightened obligations to conduct effective clandestine collection against an adversary’s systems before initiating a cyber-attack. As an example, an attacker should know in advance whether the targeted computer network is also connected with an adjoining university and its hospital. Without an accurate digital map of an adversary’s system, the prospective attacker cannot ensure that legitimate targets are selected and targeted, and attacked in a manner to avoid unnecessary incidental injury or collateral damage to persons or infrastructure,

---

207 1979 Protocol I, supra note 33, at art. 51(5)(b). The United States recognizes the principles of distinction and proportionality to be customary international law. Matheson, supra note 33.

208 1979 Protocol I, supra note 33, at art. 57(2). The United States does not recognize this point as customary international law. See INTERNATIONAL AND OPERATIONAL LAW DEPARTMENT, LAW OF ARMED CONFLICT Documentary Supplement 234-35 (David H. Lee ed., 5th ed. 2014).

209 1979 Protocol I, supra note 33, at art. 57(3).


implicating the aforementioned principles of necessity, distinction, proportionality and humanity.

Perfidy, acts inviting an adversary’s detrimental reliance on a protected status, has been a traditional concern under IHL and takes on heightened relevance in cyber operations.\(^{213}\) The rule against perfidy prohibits a range of activities including the feigning of surrender, incapacitation, civilian status, or a protected status involving the “signs, emblems or uniforms” of U.N. personnel or neutral parties with an intent to betray that confidence,\(^{214}\) as well as the use of neutral flags, emblems, insignia or uniforms, or that of the enemy while engaging in attacks.\(^{215}\) In contrast, ruses, which are not prohibited, are defined as acts intended to mislead or deceive an enemy, but do not misuse a protected status or symbol.\(^{216}\) Yet, how can a cyber-attack constitute an act of perfidy, as opposed to a lawful ruse? Professor Sean Watts, a law professor at Creighton University and Judge Advocate General Corps officer in the U.S. Army Reserve, contends that:

“While cyber-attacks appear in a variety of forms—many involving little if any overt deception or misrepresentation—the potential for misrepresentations, deceit, and resulting distrust abounds. More important, cyber hostilities illustrate clearly the potential for harm achieved by deception to undermine confidence in a vital mode of human interaction.”\(^{217}\)

In a sense, all covert operations involve some level of secrecy and deception, largely in an effort to gain a decision advantage over an adversary. A digital attacker does not distinguish himself as a “combatant,” making it difficult for a defender to know whether a transmission (e.g., the data contained on a thumb drive) has civilian status. It could, for example, violate the rule against perfidy by using a thumb drive, disk or other device that is marked as “U.N. Inspections Guide,” “medical,” or an update to a popular iTunes app. On the other hand, it might be an acceptable ruse to mark the bait as “engineering texts,” “tools program,” or a Windows update. In a certain sense, the rule against perfidy seems like an anachronism, reminiscent of the pre-cyber battlefields, especially when one considers that the rule developed because of actions such as the misuse of a white flag of surrender or the use of a medical vehicles to mount a direct and kinetic attack. Nonetheless, except for the AP I, Article 37 (c), prohibition against “the feigning of civilian, non-combatant status,” perfidy should not be a significant problem for cyber practitioners.

\(^{215}\) *Id.* at art. 39.
\(^{216}\) *Id.* at art. 37(2).
\(^{217}\) Watts, *supra* note 213, at 115.
E. Conclusions on International Law

International law imposes important constraints on the use of force in international relations. Cyber-attacks, kept below a certain threshold of harm and narrowly focused on discrete objectives, such as disabling an illegal nuclear weapons program, might not be considered as a “use of force,” much less an “armed attack,” under international law. Nonetheless, a victim state faces significant problems in characterizing and attributing an event, suggesting that covert cyber actions might be a preferred tool for policymakers. Indeed, covert cyber operations have a certain appeal for technologically advanced countries such as the United States or Israel: cyber operations can minimize the risk of friendly casualties and leave the victim-state with a difficult dilemma: admit that an attack occurred, causing some level of domestic embarrassment at an inability to defend sensitive national systems, or make an accusation that might not be provable based problems with attribution.

FINDINGS AND IMPLICATIONS

Offensive cyberspace operations, particularly certain exploitative and covert activities, violate international norms, or at least the norms against intervention and interference in the domestic affairs of foreign sovereign powers, and may result in international responsibility for wrongful acts. Nonetheless, covert cyber action is a viable foreign policy tool for U.S. policymakers and national security practitioners, subject to important direction and control by the executive branch and under the lamp of congressional oversight. In cases where the President acts consistent with his constitutional duties and statutory authority, executive power is “at its maximum.” Thus, the critical issue is not whether a covert action is legal in a domestic sense or whether it should be used to further our strategic policy objectives. Rather, the debatable issues center on when, where, how, and under what direction and control such operations should be conducted. In turn, this raises questions regarding possible impact on U.S. national interests, especially as it relates to compliance with the rule of law and any perceived consistency/inconsistency between stated values and state practice. In cases where the executive branch assesses a requirement for this unique capability, it must proceed in a way that maximizes the benefit to U.S. interests, protects against the unwarranted abuse of civil liberties, and minimizes the risk to intelligence practitioners of foreign capture and prosecution.

There are multiple areas of tension involving executive direction and control on one hand, and congressional oversight on the other. The blurring of lines between intelligence and military activities, especially as it relates to covert actions, has caused increased problems in executive accountability and

218 G.A. Res. 2131(XX), Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty (Dec. 21, 1965).

219 Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635 (1952) (Jackson, J., concurring).
congressional oversight. Offensive cyberspace actions, including both cyber exploitation and attack, should be construed as a covert activity and not subject to the statutory exception for “traditional military activities.”\textsuperscript{220} In a certain sense, it probably does not matter whether the cyber warrior is uniformed military or a civilian, provided that there is a clear oversight within the executive branch and by the relevant congressional committees. Clear presidential control is essential, especially if the covert action can have a crippling effect or may be seen as an act of war by an adversary. It matters greatly that the supervisory chain has professional expertise in managing covert actions and in supervising the myriad of technical issues that must surely arise. Thus, where military personnel support or take part in a covert action, congressional oversight should be expanded to include members of the Senate and House Armed Services Committees. Congress should clarify the appropriate roles and missions of the CIA, the NSA, and the U.S. CYBERCOM.

The U.S. government must conduct offensive cyberspace operations in coordination with our foreign policy goals and objectives, furthering national interests such as security against foreign actors while promoting U.S. values such as the rule of law. To accomplish this, the Senate Foreign Relations Committee, the House Foreign Affairs Committee, and the Department of State should be “fully and currently informed”\textsuperscript{221} about planned intelligence operations abroad. U.S. ambassadors, in their Chief of Mission capacity, must also be “fully and currently informed,” preferably by the Director of National Intelligence, about prospective operations with sufficient advance notice to offer recommended changes and provide the required “direction, coordination, supervision of all Government executive branch employees in that country ….”\textsuperscript{222} Clearly, U.S. Foreign Service professionals, to include Chiefs of Mission, are often in the best position to assess how a proposed covert action, either passing through or conducted in a country, will affect the bilateral relationship.

Offensive cyberspace operations should be narrowly focused to achieve objectives consistent with deeply held international norms. Thus, where a cyber action furthers the cause of international peace and security by undermining an illegal weapons (nuclear or chemical) program, by sending a deterrent message to a rogue nation that has been making illegal threats of force against its neighbors, or in impairing a non-state actor that has been inciting acts of terrorism, the action is more likely to be seen as legitimate by the international community. This is especially true where the cyber action falls below either the threshold for the “use of force” in Article 2(4) or for “armed attack” in Article 51 under the U.N. Charter. A cyber action can be the ultimate “frontier incident” that leaves the victim with impossible problems in characterizing and attributing the attack to the responsible parties, and with not knowing when or where the

\textsuperscript{221} 22 U.S.C. § 3927(a) (2019).
\textsuperscript{222} \textit{Id.}
next attack might come. Finally, the basic principles of IHL, to include necessity, distinction, proportionality, and humanity does not necessarily cabin the legality of cyber operations, but should inform the planning and execution of any such action for U.S. officials.